Avaya Application Solutions:
IP Telephony Deployment Guide

555-245-600
Issue 6
January 2008

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the documents, *Avaya Support Notices for Software Documentation*, 03-600758, and *Avaya Support Notices for Hardware Documentation*, 03-600759.

These documents can be accessed on the documentation CD and on the Web site, http://www.avaya.com/support. **On the Web site, search for the document number in the Search box.**

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support.

Contents

About This Book

Overview

This book, *Avaya Application Solutions IP Telephony Deployment Guide*, 555-245-600, describes Avaya's Application Solutions product line, IP Telephony product deployment, and network requirements for integrating IP Telephony products with an IP network. The guide can be used as a tool to provide a better understanding of the benefits of Avaya IP solutions and of the many aspects of deploying IP Telephony on a customer's data network.

This book does not contain procedural information for installing, configuring, or maintaining IP telephony products. This type of procedural information is contained in other product documentation available at http://www.avaya.com/support.

Audience

The primary audiences for this book are:

- Avaya employees and Business Partners working in sales and sales-support organizations.
- Customers considering the purchase of Avaya's IP Telephony products.
- Avaya customers who have purchased IP Telephony products and are seeking suggestions for their implementation.

Secondary audiences include the Technical Service Center (TSC), training, and development.

Using this book

This book is organized in three major sections:

Section I - Avaya Application Solutions product guide. Use this section to learn about Avaya's IP Telephony products including:

- Communication Manager
- Servers and gateways and their configurations and capacities
- Migration from circuit-switched to packet-switched products

- Call processing features
- LAN switching products

Section II - Deploying IP Telephony. Use this section to learn about deployment issues including:

- Traffic engineering
- Security
- Voice quality issues
- Network management
- Reliability and recovery

Section III - Getting the IP network ready for telephony. Use this section to learn about preparing an IP network for telephony, including:

- Network design and engineering
- Quality of service
- Network recovery
- Network assessment

Appendix A - covering Converged Network Analyzer configuration.

Downloading this book and updates from the Web

You can download the latest version of the *Avaya Application Solutions IP Telephony Deployment Guide,* 555-245-600, from the Avaya Support Web site. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site might also contain new product information and updates to the information in this book. You can also download these updates from the Avaya Web site.

To download the latest version of this book:

1. Access the Avaya web site at http://www.avaya.com/support.
2. On the upper left of the page, type **555-245-600** in the Search Support box, and then click **Go**.

   The system displays the Product Documentation Search Results page.
3. Scroll down to find the latest issue number, and then click the book title that is to the right of the latest issue number.

Related resources

For more information on Avaya IP Telephony products, see the following documentation libraries and CDs:

Title	Number or Link
Documentation for Avaya Communication Manager Release 3.1, Media Gateways and Servers	03-300151
Avaya Communication Manager Quick Reference Set	03-300366
Avaya IP Telephony Implementation Guide	iImplementation_Guide
Documentation Ordering Instructions	03-300440

Technical assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with:

- Feature administration and system applications, call Technical Consulting System Support (TCSS) at 1-800-225-7585
- Maintenance and repair, call the Avaya National Customer Care Support Line at 1-800-242-2121
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353

International

For all international resources, contact your local Avaya authorized dealer.

Trademarks

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Sending us comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

  Avaya Inc.
  Product Documentation Group
  Room B3-H13
  1300 W. 120th Ave.
  Westminster, CO 80234 USA

- E-mail, send your comments to:

  document@avaya.com

- Fax, send your comments to:

  1-303-538-1741

Ensure that you mention the name and number of this book, Avaya Application Solutions IP Telephony Deployment Guide, 555-245-600.

Section 1: Avaya Application Solutions product guide

Avaya Application Solutions

This chapter contains general discussions of the Avaya Application Solutions product line:

- Avaya Communication Manager
- Avaya servers
- Avaya DEFINITY Servers
- Avaya Media Gateways
- Avaya Integrated Management
- Avaya Communication Manager applications
- Avaya SIP solutions
- Avaya SIP application enablement

The next-generation Avaya Application Solutions portfolio powered by Avaya Communication Manager delivers on the promise of IP by offering a no-compromise approach to convergence in terms of reliability and functionality. “No compromise” means that Avaya allows customers to migrate to IP Telephony without compromising on features (all features are maintained or expanded), interfaces (all existing telephones and lines are supported, along with new IP Telephones, Softphones, and IP trunks), or reliability. Avaya Communication Manager is the centerpiece of Avaya Application Solutions.

Communication Manager runs on a variety of Avaya servers, provides control to Avaya Media Gateways and Avaya Communications Devices, and can operate in a distributed or network call processing environment. Figure 1: Avaya Application Solutions on page 17 and Figure 2: Communication Manager traffic flow on page 18 summarize the Avaya Application Solutions.

Figure 1: Avaya Application Solutions

Figure 2: Communication Manager traffic flow

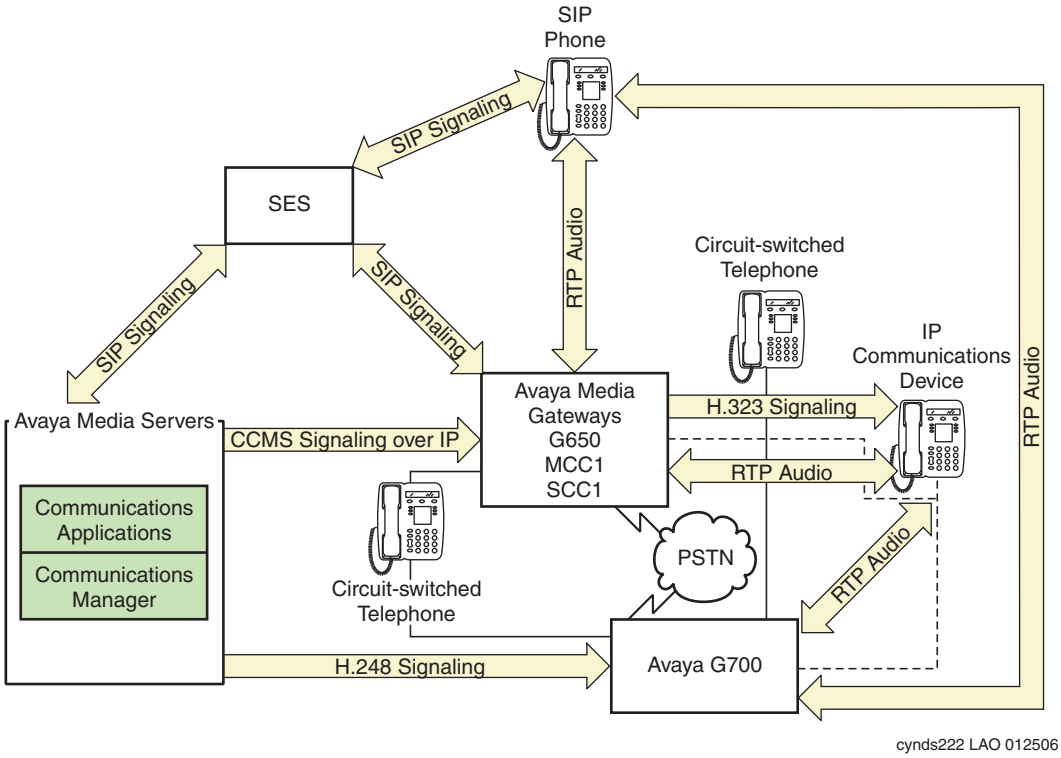


Figure notes:

1. **SIP phones exchange RTP audio among themselves and with the G700, G650 Media Gateways, and so forth, but not with IP phones.**
2. **SIP signaling from Avaya Communication Manager is always to/from SES.**
3. **SIP signaling can go through a C-LAN (on a G650, etc.), or directly Communication Manager (if the server is the S8300 or S8500).**

Note:

This is actually true for both H.323 and H.248 signaling. The diagram gives the impression that H.248 comes directly from Communication Manager and H.323 goes through the media gateways, when in fact both protocols can go both ways depending on server type.

Communication Manager is the next generation of Avaya call processing software. Communication Manager is an open, scalable, highly reliable, and secure telephony application. Communication Manager operates on Avaya servers, and on the existing family of DEFINITY servers.

Communication Manager carries forward all the current DEFINITY capabilities, plus all the enhancements that enable enterprises to take advantage of new, distributed technologies, increased scalability, and redundancy. Communication Manager is evolved from DEFINITY software and delivers no-compromise, enterprise IP Telephony.

Avaya Media Gateways support voice traffic and signaling traffic that is routed between circuit-switched networks and packet-switched networks. The Gateways support all the applications and adjuncts that can be used with the Avaya DEFINITY Enterprise Communications Servers (DEFINITY ECS). These Gateways work with standards-based data networks and easily connect with the Public Switched Telephone Network (PSTN).

Communication Manager is extensible to IP, digital and analog telephones, and wireless business solutions. Avaya Communication Devices work with the full feature set of Communication Manager to help enterprises be more productive by providing anytime, anywhere access to maximize business continuity.

Avaya Communication Manager

Avaya Communication Manager provides user and system management functionality, intelligent call routing, application integration and extensibility, and enterprise communications networking. Communication Manager operates on Avaya servers, and on the existing family of DEFINITY servers. For more information on the Avaya Application Solutions related features of Communication Manager, see Call processing on page 125.

Avaya servers

An Avaya server provides centralized, enterprise-class call processing. This call processing can be distributed across a multi-protocol network (including IP) to support a highly diversified network architecture that consists of headquarters, branch, remote, small, and home offices.

Linux-based servers

The Avaya S8300, S8400, S8500, S8700-series, and SES-SIP are Linux-based servers. These servers support:

- Distributed IP Networking and centralized call processing across multi-service networks
- Dual server design with hot fail-over (S8700-series Server only)
- Redundant LAN Interfaces and remote survivable call processing

For more information on the architecture and the functionality of the servers, see *Hardware Description and Reference for Avaya Communication Manager,* 555-245-207.

Avaya DEFINITY Servers

Avaya Communication Manager also runs on the following DEFINITY Servers, which can be IP-enabled:

- Avaya DEFINITY Server R
- Avaya DEFINITY Server SI
- Avaya DEFINITY Server CSI

These servers run on the Oryx/Pecos proprietary operating system, and function in the same way as the servers in Figure 2: Communication Manager traffic flow on page 18. These servers fit into Avaya CMC1, SCC1, and MCC1 Media Gateways.

The focus of this document is network design incorporating the newer Communication Manager platforms. Therefore, the DEFINITY Servers are only discussed briefly here.

Avaya Media Gateways

An Avaya Media Gateway supports both bearer traffic and signaling traffic that is routed between packet-switched networks and circuit-switched networks. Communication Manager running on Avaya servers controls voice and signaling over a variety of stackable and modular Media Gateways:

- Avaya G150 Media Gateway
- Avaya G250 Media Gateway
- Avaya G350 Media Gateway
- Avaya G450 Media Gateway
- Avaya G650 Media Gateway
- Avaya G700 Media Gateway
- Avaya G860 High Density Media Gateway
- Avaya CMC1 Media Gateway
- Avaya SCC1 Media Gateway
- Avaya MCC1 Media Gateway
- MultiTech MultiVoIP Gateway
- Avaya IG550 Integrated Gateway

The Media Gateways contain the network and the endpoint interfaces, as well as call classification, announcement boards, and so on. Through these interfaces, Communication Manager performs gateway/gatekeeper functions. For more information on the Media Gateways, see Small to mid-size enterprise on page 37 and Mid-market to large enterprise on page 79.

Avaya Integrated Management

Avaya Integrated Management is systems-management software for managing converged voice and data networks.

The Integrated Management applications include the tools that enable you to

- configure, monitor, and optimize the performance of Avaya servers, gateways and
- endpoints
- monitor voice over IP traffic
- manage Quality of Service (QoS) policies
- control network quality

For more information on Avaya Integrated Management, see:

- Avaya Integrated Management on page 257

Avaya communication devices

Avaya Communication Manager provides intelligent control for a variety of smart communication devices, including the one-X Deskphone family of IP telephones, IP Softphones, digital telephones, attendant consoles, analog telephones, and wireless telephones. For information on these devices, see *Hardware Description and Reference for Avaya Communication Manager*, 555-245-207.

Avaya Communication Manager applications

Avaya Communication Manager supports the following communication capabilities and applications:

- Call Center
- Messaging
- Unified Communication Center
- Avaya Call Management System (CMS)
- Conferencing systems
- Meet-me conferencing
- Avaya Meeting Exchange Solutions
- Video Telephony Solutions
- Computer Telephony Integration (CTI)
- Application Programming Interfaces (APIs)
- Best Services Routing (BSR) polling

For more information on these applications, see Communication applications on page 152 and http://www.avaya.com/support.

Avaya SIP solutions

Session Initiation Protocol (SIP) is an endpoint-oriented messaging standard defined by the Internet Engineering Task Force (IETF). SIP is a text-based protocol, similar to HTTP and SMTP, for initiating interactive communication sessions between users. Such sessions include voice, video, instant messaging, interactive games, and virtual reality.

As implemented by Avaya for Communication Manager release 3.0 and beyond, SIP "trunking" functionality is available on any of the Linux-based servers (S8300, S8400, S8500 or S8700-series). SIP trunking allows Avaya Communication Manager to communicate with SIP endpoints and gateways across an IP network. SIP trunks allow an enterprise to connect its server(s) to an Avaya SIP-Enablement Server (SES), a SIP-enabled proxy server, and through this proxy to an external SIP service provider, if desired. The trunk support in Communication Manager complies with SIP standards, specifically IETF RFC 3261, and so interoperates with any SIP-enabled endpoint/station that also complies with the standard.

Avaya Communication Manager supports SIP endpoints, including the Avaya 4602 SIP Telephone and Avaya IP Softphone Release 5. In addition to its IP telephony capabilities, IP Softphone R5 also includes Instant Messaging (IM) client software, which is a SIP-enabled application that connects to the SES for IM control. By means of having SIP-enabled endpoints managed by Communication Manager, many features can be extended to these endpoints.

Avaya SIP application enablement

Avaya Communications Process Manager is middleware software that uses customizable web services to integrate Avaya communications solutions into customer business processes. Communications Process Manager achieves this integration by detecting events from a customer business application. Different events trigger Communications Process Manager to invoke different communication applications to escalate the situation to people and resources that can address it.

Communications Process Manager performs the following functions:

- Integrates the following Avaya communication resources. This integration makes it possible for the resources to communicate with Communications Process Manager and ultimately with each other.
  - Communication Manager — provides telephony capabilities.
  - SIP Enablement Services (SES) — serves as the SIP proxy. All communication resources use SIP to communicate through Communications Process Manager.
  - Meeting Exchange Express — provides audio conference capabilities.
  - Voice Portal — provides interactive voice response (IVR) capabilities for phone interactions between Communications Process Manager and its users.
- Orchestrates interactions between the communication resources.

- Exposes composite communication service units expressed in the form of generic web service constructs understood by the business community at large.
- Uses presence and availability computations to route communication to the right device of the user.

Communications Process Manager makes it possible for customers to combine their data related activities with communication to:

- Rapidly mobilize the right people for decision making (no matter where they are, or on what device)
- Significantly reduce the human latency required today in contacting people
- Incorporate automatic alerts into business process decisions.

Communications Process Manager uses internal service-oriented architecture (SOA) with both loose coupling between its internal components and a scriptable orchestration engine. This architecture provides a high degree of customizability and very loose coupling between the customer business processes and the communications systems that are used to implement the Communications Process Manager Web services. The various components of Communications Process Manager can be included or excluded to meet customer needs.

Avaya Distributed Office

Note:

See www.avaya.com/support for a complete set of documentation for Avaya Distributed Office.

As enterprises evaluate replacements for traditional Key-Hybrid telephone systems at the branch, they must carefully consider investments that reduce total cost of ownership, lower operational expenses, and enable better interaction with customers.

Distributed Office provides large and medium multi-site enterprises an elegant migration from branch-office Key-Hybrid systems to an IP-based solution. Distributed Office is a distributed and scalable Session Initiation Protocol (SIP) solution that delivers local telephony and communications applications to multiple locations. Target markets include financial services outlets, retail stores, transportation depots, and regional offices for government and other industries. Replace variable w/ short product name supports centralized administration and can be rapidly deployed as either individual branch locations or as a network of branch locations. Distributed Office is based on open standards using SIP and Web-Services for maximum investment protection.

This highly available solution does not depend on WAN health for local branch operation because call processing is distributed to each branch location. Yet customers can still link branches together, routing voice, presence, and instant messaging, and also leverage connections to corporate headquarters to provide enhanced customer service.

Avaya Distributed Office contains integrated features, applications, and much more. At each branch location, Distributed Office is implemented in one of two platforms — Avaya Distributed Office i40 or Avaya Distributed Office i120. These platforms are available in numerous configurations.

Distributed Office Configurations

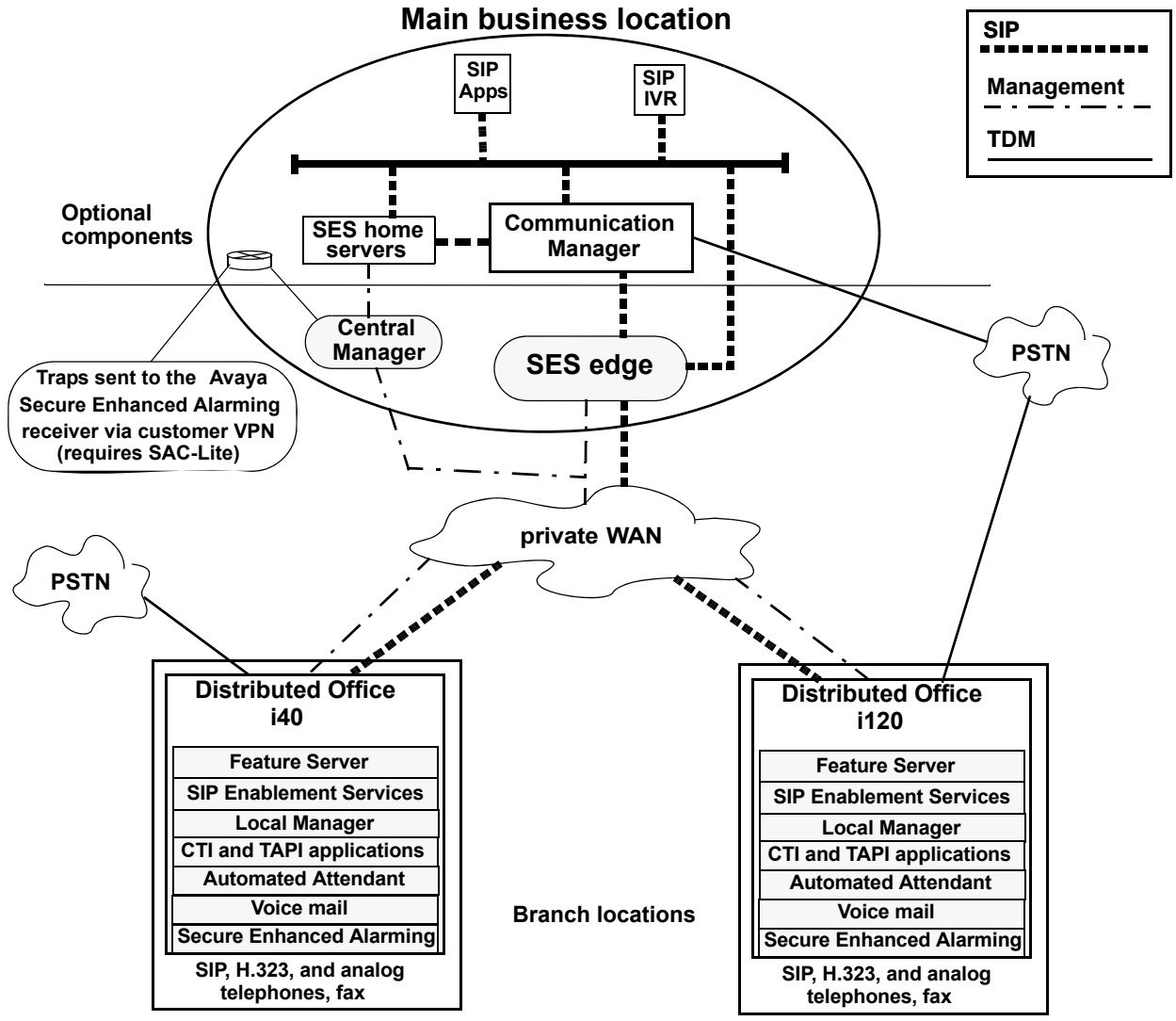
An Avaya Distributed Office system can be configured as

- an individual branch location
- an individual branch location with centralized management
- a Networked branch location

The diagram in Figure 3 shows a Distributed Office solution with networked branch locations. This configuration supports:

- SIP calls between the branch and main locations over the private WAN or public Internet.
- Inter-branch SIP calls through an SIP Enablement Services (SES) edge proxy at the main location.
- Integrated Management for Distributed Office at the main location provides centralized management to the branch locations.
- Optional connection to Communication Manager server through the SES home proxy.

Figure 3: Networked remote sites



Distributed Office benefits

The benefits of Avaya Distributed Office include advanced functionality such as:

- Platform features
  - Feature server including both PBX and Key-System features
  - SIP Enablement Services
  - Voice Mail
  - Announcements
  - Auto attendant
  - Call Detail Recording
  - Secure Enhanced Alarming
- Application Enablement Services
  - Extend Avaya's rich features in an IP environment to get the most from your current investment.
  - Integrate communications & business applications to leverage existing infrastructure and maximize efficiency.
  - Support some third-party application integration to provide mission-critical support for key business processes.
  - Computer-telephony integration services.

Distributed Office implementation

The Distributed Office solution provides a set of standard hardware configurations or *constructs* and set of provisioning *profiles*. A construct is chosen that best satisfies the hardware requirements for one ore more locations. A provisioning profile, consisting of a set of files containing provisioning data, is selected and loaded onto the hardware platform.

Selecting a construct

When you use the Avaya Solution Designer to create a configuration template for a group of branch locations, the choice of a construct is the most important parameter. The choice of construct determines the number of lines and trunks of each type. The goal is to choose the smallest construct that accommodates the maximum requirements assuming growth.

The first consideration when choosing a construct is the Distributed Office model, i40 or i120. A construct that uses the i120 model provides a larger number of lines and trunks than the i40, as well as higher capacities for several other parameters such as the number of voice mail boxes, the number of DSPs, and the busy hour call completion rate.

An i40 might provide an adequate number of lines and trunks for the current business requirements but not for increased requirements in two years based on growth assumptions. Or, an i40 might provide enough lines and trunks for the next several years but another parameter, such as the number of DSPs to handle large Fax volumes might not be sufficient. In either case, one of the i120 constructs would be a better choice.

Table 1: i40 constructs on page 27 and Table 2: i120 constructs on page 29 provide the information needed to choose a construct.

Note:

The list of available constructs might change over time. Check on the Avaya Distributed Office web site for the latest set of available constructs.

i40 constructs

Each i40 construct contains the following ports:

- One console cable port
- One interface USB port (located on the chassis where you connect the Disk on Key)
- One Contact Closure Adjunct (CCA) port
- One Ethernet WAN port (not used with Distributed Office)
- Eight Ethernet LAN Power over Ethernet (PoE) ports
- One USB port (for use with a USB modem for servicing the platform)
- One Ethernet services port
- Two analog line ports

In addition to these ports, the i40 contains additional ports based on its construct. Table 1 shows the three i40 constructs, and a description of what additional ports are available for each.

Table 1: i40 constructs

Construct	Analog trunk ports	ISDN BRI trunk ports	T1/E1 interface port[1]
i40 - Analog	4		
i40 - BRI	1	2	
i40 - DS[2]	1		1

1. The T1/E1 interface port can be configured for ISDN PRI, Robbed Bit, or CAS signaling.

2. The i40 - DS1 construct also contains three pairs of test jacks that are used by service personnel only.

i120 constructs

Each i120 construct contains the following ports:

- One analog trunk port
- Two analog line ports
- One Contact Closure Adjunct (CCA) port
- One Ethernet WAN port (not used with Distributed Office)
- One Ethernet LAN PoE port
- One console cable port
- One interface USB port (located on the chassis where you connect the Disk on Key)
- One USB port (for use with a USB modem for servicing the platform)
- One Ethernet services port

Note:

If you need additional ports, additional Media Modules are available for the i120 platform constructs. See your Avaya representative for details.

In addition to these ports, the i120 contains additional ports based on its construct. Table 2 shows the ten i120 constructs, and a description of what additional ports are available for each. The legend for the various construct names is a follows:

Legend:

A = Analog (RJ-11, 2-wire)
B = BRI
D = Digital (DS1, T1, E1, and PRI)
H = High Capacity (24 analog ports using a single connector)
P = Power over Ethernet (PoE)

Table 2: i120 constructs

Construct	Analog ports for lines or trunks	Analog line ports	10/100 Ethernet Base-T PoE ports	T1/E1 interface port[1]	ISDN BRI trunk ports
i120 - A	8				
i120 - AH	8	24			
i120 - A2H	8	48			
i120 - AP	8		40		
i120 - 2AP	16		40		
i120 - D2H[2]	8	48		1	
i120 - DP[2]	8		40	1	
i120 - BH	8	24			8
i120 - B2H	8	48			8
i120 - BP	8		40		8

1. The T1/E1 interface port can be configured for ISDN PRI, Robbed Bit, or CAS signaling.

2. The i120 - DH and i120 - DP constructs also contains three pairs of test jacks and a connector that are used by service personnel only.

Distributed Office application module and media modules

Avaya AM110 Application Module

The Avaya AM110 Application Module is the heart of the Replace variable w/ short product name system. The AM110 Application Module provides the telephony features, voice mail, automated attendant, SES, and TAPI. The AM110 Application Module also contains a Freescale processor and replaceable Compact Flash and SO-DIMM memory.

The AM110 Application Module is included with both the i40 and i120 platforms. The Avaya AM110 Application Module can be inserted only in slot V1 of either the i40 or the i120.

Telephony media modules

The ten constructs for Distributed Office i120 contain one or more media modules. Table 3 shows the available media modules, and the slot or slots in which each module can be inserted.

Table 3: Supported media modules

Module	Description	Permitted slots
Telephony modules		
MM710	One T1/E1 ISDN PRI trunk port	V2, V3, V4, V5
MM711	Eight universal analog ports	V2, V3, V4, V5
MM716	Twenty-four analog line ports	V2, V3, V4, V5
MM720	Eight ISDN BRI trunk ports	V2, V3, V4, V5
LAN module		
MM316	Forty 10/100 Ethernet ports with Power over Ethernet (PoE), and one 10/100/1000 Ethernet copper uplink/access port	V6

Streamlined Deployment

A major goal of the Distributed Office offering is to minimize the time to deploy the Distributed Office systems at the branch locations. The total deployment time includes:

- Unpacking, assembling, and cabling the hardware
- Enter site-specific and other dynamic data
- Acceptance testing

The first and third deployment items require a fixed amount of time for each construct. The time required for the second item, completing the provisioning data, varies according to the amount of data that needs to be added or changed in the profile that was loaded onto the system or onto a USB portable storage device, or "Disk on Key" (DoK).

The design activities described previously determine the type and the number of the Distributed Office hardware components for each branch location. The implementation process then uses data files called *profiles* to load the translations and other parameter values onto the i40 or i120 Distributed Office platform before it is shipped to the customer site.

In the design phase, the Sales Engineer uses the Avaya Solution Designer to create a purchase order that specifies the Distributed Office hardware for each branch location. For each branch location or group, the Sales Engineer specifies that the provisioning profile is:

- Standard — The profile is one of a set of profiles that have been previously defined and associated with a hardware construct.

- Custom — The profile is not a Standard profile and needs to be created.
- None (Default)— The default profile associated with the hardware construct will be shipped and the provisioning data will be entered when the system is installed.

The deployment of a Distributed Office system is called "configure-to-order" if the provisioning profile is standard or custom. The deployment is called "made-to-stock" if the default profile is shipped. For a configure-to-order deployment, some or all of the customer-specific provisioning data is loaded onto the Distributed Office platform and all of the system components are assembled and tested before it is shipped to the customer site. A configure-to-order deployment minimizes or eliminates the implementation tasks at installation time.

For a made-to-stock deployment, no customer-specific provisioning data is associated with the Distributed Office system before it is shipped to the customer site. The system components are shipped separately from one or more distribution points. The made-to-stock platform contains a default profile that provides a minimal amount of provisioning data that is needed for the hardware construct.

Provisioning status

The provisioning status of a Distributed Office system when it is shipped to the customer location is one of the following:

Fully configured. Minimum additions or changes to the provisioning data. Use Local Manager to check the data.

Partially configured. Some additions or changes to the provisioning data. Use the Profile-based Setup Assistant to add or change the dynamic portion of the provisioning data.

Configure from scratch. All provisioning data must be entered. Use the Initial Setup Assistant to make the system operable. Then use Local Manager to enter the provisioning data.

Fully configured systems

For a fully configured system, all of the provisioning data, including location-specific data, has been obtained from the customer and loaded onto the i40 or i120 Distributed Office module before shipment to the branch location. At installation, only the hardware assembly and acceptance testing is required.

Typically, there will be some minor additions or adjustments to the provisioning data. This can be done either locally, using the Local Manager application, or remotely, using the Distributed Office Central Manager.

Partially configured systems

For a partially configured system, a Standard profile is selected or a Custom profile is created that contains some of the provisioning data. The profile contains a section for dynamic data, which is either missing and needs to be added or is temporary and needs to be confirmed or changed. The partially configured profile is either loaded onto the i40 or i120 Distributed Office module or copied to a USB portable storage device before shipment to the branch location.

A Profile-based Setup Assistant is created as part of the profile. At installation, the Assistant prompts the installer to add or change the dynamic data.

From-scratch configuration

If none of the profiles, including the default profile, is appropriate, the system can be reset to its initial configuration by executing the **`nvram init`** command. In this case the Initial Setup Assistant is used to enter the minimum provisioning data to make the system operable. Then the remaining provisioning data is entered using Local Manager.

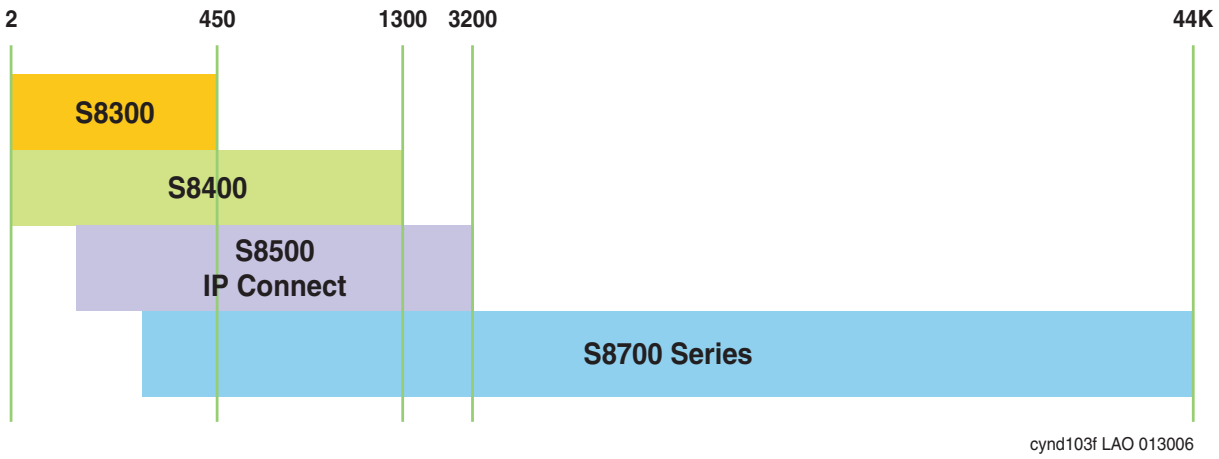
Avaya Application Solutions platforms

Overview

The Avaya Communication Manager portfolio covers small, medium, and large enterprises with advanced communications needs between 2 and 48,000 ports per system. This chapter provides an overview of the Avaya Communication Manager platforms architecture that supports Avaya Application Solutions components and features.

Figure 4 shows the approximate port capacities for Avaya's Application Solutions platforms.

Figure 4: Avaya Application Solutions platforms port capacities



An overview of the properties of the Avaya servers described in this chapter is provided in Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities on page 34.

Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities[1]

	Avaya S8300 Server	Avaya S8400 Server	Avaya S8500 Server	Avaya S8700-series Server
Processor/ RAM/ disk drive	Intel Celeron class server 512 MB of RAM 30 GB hard disk drive	Intel Celeron M 512 MB RAM 30 GB hard disk drive 2 GB Solid State Disk (SSD)	Intel Pentium IV Class Server 512 MB of RAM 80 GB hard disk drive Removable Flash card backup	**S8710:** Intel Pentium IV Class Server 512 MB RAM 72 GB disk drive Removable Flash card backup **S8720:** AMD Opteron 1 GB RAM 72 GB disk drive Removable Flash card backup **S8730:** AMD Dual Core Opteron 4 GB RAM 72 GB disk drive
General Business analog equivalent BHCC rate	10,000	10,000	100,000	**fiber-PNC:** 400,000 180,000 IP station to trunk calls 80,000 H.248 media gateway calls 25,000 SIP calls **IP-PNC:** 180,000
Maximum Telephones (IP + non-IP)	S8300: 450 S8300/G700: 450 S8300/G450: 450 S8300/G350: 40 S8300/G250: 12	900	2,400	36,000
Maximum Trunks (IP + non-IP)	S8300: 450 S8300/G700: 450 S8300/G450: 450 S8300/G350[2]: 40 S8300/G250: 10	400	800	8,000 Total up to 5,000 can be SIP For XL configuration: 12,000 Total

1 of 2

Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities[1] (continued)

	Avaya S8300 Server	Avaya S8400 Server	Avaya S8500 Server	Avaya S8700-series Server
Maximum IP Endpoints (IP Telephones + IP Trunks)	S8300: 900 Total S8300/G700: 900 Total 450 Trunks 450 Telephones S8300/G450: 900 Total 450 Trunks 450 Telephones S8300/G350: 55 Total 15 Trunks 40 Telephones S8300/G250: 20 Total 10 Trunks 10 Telephones	1,300 Total 400 Trunks 900 Telephones (450 can be SIP)	3,200 Total 800 Trunks 2,400 Telephones (all can be SIP)	12,000 Total (all can be SIP) For XL configuration: 16,000 Total (12,000 can be SIP) 8,000 Trunks For XL: 12,000 Trunks
Maximum Subtending Media Gateways	S8300/G700/G450: 50 H.248 S8300/G350/G250: subtending gateways not supported	5 H.248 A single PN composed of: 1–5 G650s 1–3 G600s 1–4 CMC1s	250 H.248 3 MCC1 or SCC1 PNs Direct connect 64 G650 PNs (IP-PNC)	250 H.248 **fiber-PNC:** 44 MCC1 or SCC1 PNs with CSS 64 MCC1 or SCC1 PNs with ATM **IP-PNC:** 64 G650 PNs
Maximum Media Gateways per LSP	50 per S8300 LSP	5 per S8300 LSP	250 per S8500 LSP 50 per S8300 LSP	250 per S8500 LSP 50 per S8300 LSP
Reliability / survivability	LSP SLS[3]	LSP for G700/G450/ G350/G250	LSP backup for G700, G450, G350, or G250 S8500 ESS	Duplicated Processor LSP backup for G700, G450, G350, or G250 S8700-series ESS S8500 ESS Duplicated control network Duplicated bearer connectivity
Sockets on Processor Ethernet interface	1,700	1,700	2,500	NA

2 of 2

1. The operating system for all servers is Linux (Red Hat Enterprise Linux 4.0).

2. S8300/G350 trunks either H.323 or SIP. Up to 15 IP trunks
3. Each G250 has built-in Standard Local Survivability (SLS) that provides basic services for local IP and non-IP phones and PSTN trunks. The G150 also has built-in survivability with features similar to those of the IP Office communication product, on which the G150 is based.
4. H.248 Media Gateways include G250, G350, IG550, G700 and G450.

Terminology

The terms *IP-PNC* and *fiber-PNC* are used in this chapter to distinguish between the two types of port network connectivity (PNC). Synonyms are *IP-connected* and *Fiber-connected*, respectively.

Fiber-connected port networks (fiber-PNC) transport bearer traffic (voice, fax, video) between PNs over fiber-optic cables using circuit-switched (TDM) protocol. IP-connected port networks (IP-PNC) transport bearer traffic over Ethernet cables using packet-switched Internet Protocol (IP). Starting with Communication Manager release 3.0, both types of port network connectivity can be combined in the same system. This allows a system to be converted from fiber-PNC to IP-PNC gradually, one port network at a time, if desired.

Note:

The term *fiber-PNC* is used in this document with almost the same meaning as the term *multi-connect*, which, in addition to fiber-connected PNs to carry the bearer traffic, implies a dedicated control network. The term *fiber-PNC* applies to configurations with either a dedicated on non-dedicated control network.

There are three kinds of fiber-PNC configurations:

Direct connect - One port network (PN), the "control PN," is IPSI-connected to the control network and one or two additional PNs are fiber-connected to the control PN. The call controller can be an S8500 Server or an S8700-series Server pair. The fiber connections are between the expansion interface (EI) circuit packs (TN570) in the PNs.

Center Stage Switch - All PNs are fiber-connected through the center-stage switch (CSS) and one or more PNs are connected to the control network through an IPSI circuit pack (TN2312). The call controller is an S8700-series Server pair. The fiber connections are between the switch node interface (SNI) circuit packs (TN573) in the switch node carrier and the expansion interface (EI) circuit packs (TN570) in the PNs, or between SNIs in two switch-node carriers.

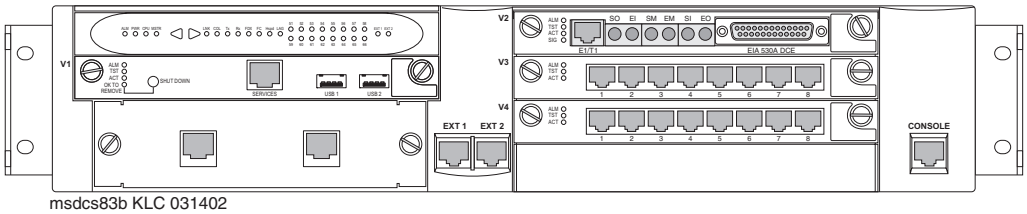
ATM - All PNs are fiber-connected through the Asynchronous Transfer Mode switch and one or more PNs are-connected to the control network through an IPSI. The call controller is an S8700-series Server pair. The fiber connections are between the ATM switch and the ATM expansion interface (ATM-EI) circuit packs (TN2305B or TN2306B) in the PNs.

Small to mid-size enterprise

Avaya S8300 Server and Avaya G700, G450, G350, or G250 Media Gateway

The S8300 Server and G700 Media Gateway solution (Figure 5: Avaya G700 Media Gateway with the S8300 Server on page 37) seamlessly delivers voice, fax, and messaging capabilities over an IP network. This unique solution converges the power of the Avaya Communication Manager feature set with the power of distributed Ethernet switching from the P330 Stackable Switching System.

Figure 5: Avaya G700 Media Gateway with the S8300 Server



The G250, G350, G700, or G450 with an S8300 as the primary controller is a stand-alone solution. The Linux-based S8300 Server can support up to 50 G250, G350, G700, or G450 Media Gateways. For more information about performance and capacities of the S8300 Server, see Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities on page 34.

An S8300 Server and G250, G350, G700, or G450 Media Gateway solution includes:

- A G700, G450, G350, or G250 Media Gateway is always required. The G700, G450, G350, or G250 hosts an S8300 Server and various media modules depending on the telephony needs at a particular location.
- The S8300 Server. The S8300 Server is inserted into a media module slot. If present, the S8300 supports Communication Manager that provides call-processing capabilities and features for the system. The S8300 can be configured as the primary call controller or as a Local Survivable Processor (LSP) standby server for another S8300 Server in the configuration.

  Note:

  The S8300 / G350 solution is intended to be a standalone solution. Multiple media gateways (either G700, G450, G350, or G250) should be controlled by an S8300 Server installed in a G700 or G450 Media Gateway.

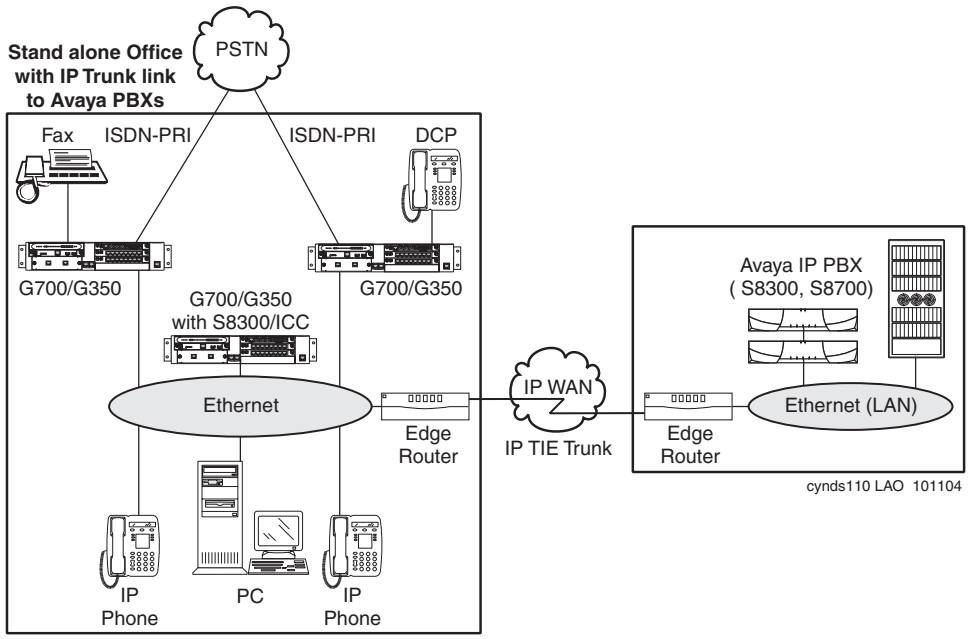
Multiple G700 Media Gateways can be connected to each other through an Octaplane 8-Gbps stacking fabric, and Avaya P330 Expansion Modules, which allows adding additional Ethernet ports, fiber interfaces, ATM access or WAN access modules without additional switches. The system can be networked to other PBXs and Communication Manager platforms through an IP network.

Some of the key characteristics of this platform are

- Expert System Diagnostic Capability
- Hot-swappable Media Modules
- Co-resident INTUITY AUDIX messaging.

The platform is scalable, and has survivability and redundancy capability through a Local Survivable Processor (LSP), which supports all of the features of Communication Manager.

Figure 6: Avaya S8300/G700, G450, G350, or G250 in a stand-alone configuration



G700 hardware architecture

The design of the Media Gateway motherboard hardware brings together a multitude of hardware functions into a single 2U 19-inch rack-mountable enclosure. Integrated on the motherboard are:

- A gateway function that bridges the IP and telephony domains
- An Ethernet switching function and associated management features through an integrated Layer 2 switch architecture
- Processing elements that are necessary to support traditional telephony interfaces, such as trunks and analog/DCP lines

These processing elements are controlled by Communication Manager, thus offering the complete set of Communication Manager call features to both IP users and traditional telephony users.

From a hardware perspective, the G700 Media Gateway is an enclosure with an internal power supply and a motherboard. This design that provides the hardware resources for the Gateway functions, and electrical connectivity for four media modules, one Cascade module, and one Expansion module. The enclosure houses the power supply and the motherboard, and provides the physical support to allow the insertion of the various modules. Figure 7: Avaya G700 Media Gateway (front view) on page 39 shows the Media Gateway enclosure.

Figure 7: Avaya G700 Media Gateway (front view)

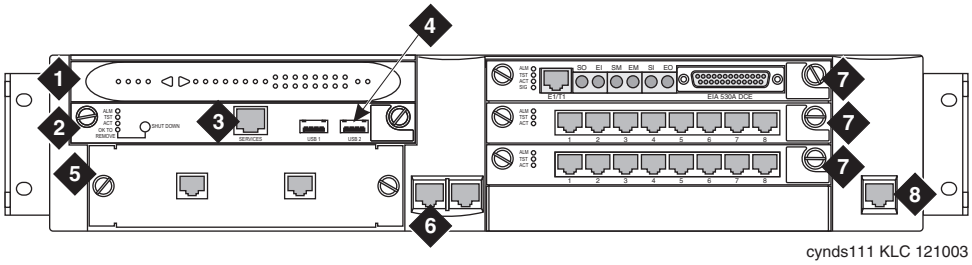


Figure notes:

1. **LED board**
2. **S8300 Server**
3. **Services port**
4. **USB ports**
5. **Avaya P330 Expansion Module**
6. **10/100 Base T Ethernet ports**
7. **Media Modules**
8. **Serial (“Console”) connector**

The four media module slots can be populated with any combination of media module types, including:

- T1/E1 with integrated CSU/DSU (MM710)
- 8-port analog line/trunk (MM711)
- 8-port DCP line (MM712)
- 24-port analog line (MM716)
- 8-port BRI trunk (MM720)
- VoIP Engine (MM760)
- Internal Communications Controller (ICC-only 1 per gateway; must be in the first slot)

The Cascade module comes from the Converged Infrastructure LAN Switches product line, and provides the Octaplane interface:

- One full-duplex 4-Gbps Ethernet port (8 Gbps bandwidth) for high-speed interconnection of up to 10 media gateways and P330 data switches in a stack arrangement
- Expansion module interface allows the use of expansion modules in the gateway. These expansion modules also allow WAN access routing.

The G700 motherboard hardware design involves three major blocks:

- A DSP engine and associated packet processor complex. This complex performs IP/UDP/RTP processing, echo cancellation, G.711 A/μ, G.729 (with or without silence suppression), fax relay, silence suppression, jitter buffer management, packet loss concealment, and so on.
- A Gateway Processor complex. This complex is the master controller of the Gateway, and controls all resources inside the Gateway under the direction of the Gateway Controller. Examples of the functions implemented here include the Media Module Manager, Tone/Clock, PKTINT, Announcements (record/playback), and H.248 signaling to the Gateway Controller.
- An Intel 960 processor complex. This complex is based on the architecture of the P330 data switch. This complex provides an eight-port Layer 2 switch function, and the i960 manages the Expansion and Cascade modules.

These major blocks are interconnected through two major communication paths: an Ethernet link and the Time Division Multiplexed (TDM) bus similar to that in a port network. In addition, the motherboard provides electrical and physical connectivity for four media modules.

VoIP Engine complex

The internal VoIP Engine block is where PCM voice samples are encoded and put into IP packets, and vice-versa. This block implements all the functions that are normally associated with a Gateway. Such functions include packet loss concealment, jitter buffer management, transcoding, and so on.

The VoIP Engine of the G700 motherboard has three major components: two Digital Signal Processors (DSPs), and a Motorola MPC8260 processor. The DSPs together provide the same VoIP channel capacities as the TN2302AP IP Media Processor circuit pack: 64 G.711 channels or 32 G.729 channels.

Each additional VoIP Media Module (MM760) increases the VoIP channel capacity of a G700 media gateway by the equivalent of a TN2302AP circuit pack.

The G700 Media Gateway Processor

The G700 Media Gateway Processor (MGP) is the master controller of the Media Gateway. The Motorola 860T processor in this complex implements the H.248 protocol to communicate with the Gateway Controller. Under the direction of the Gateway Controller, the 860T Gateway Processor controls the flow of data through the Gateway. The 860T processor communicates with other processors in the system – the VoIP Engine processor, the i960 processor, and any processors on media modules – through either the control channel of the TDM bus, or an Ethernet link (the i960 processor connects only through Ethernet).

Functions implemented within the MGP complex include:

- Management of the media modules (reset control, board and interface insertion, and so on)
- Termination of the LAPD protocol running on the D-channel of E1/T1 trunks and BRI lines and trunks (32 channels capacity).

- Recorded announcement playback (15 playback channels, 1 record channel)
- Tone detection and generation (15 ports of tone detection)
- System clock generation and synchronization to an external network timing reference
- Download agent for the media modules
- License/translation storage
- System maintenance
- H.248 signaling
- Connection management

Avaya IA770 INTUITY AUDIX Messaging Option for S8300/G700

The Avaya IA770 INTUITY AUDIX Messaging Application, (IA770), optionally embedded on the S8300 Server installed in a G700, delivers voice, fax, and e-mail to enhance and simplify the communications and the exchange of information within both small enterprises, and the smaller locations of large enterprises. The IA770 uses the Linux operating system, which is consistent with the operating system of the Media Gateway.

The IA770 supports INTUITY digital (TCP/IP) and AMIS networking protocols. More extensive networking can be provided with the Avaya Interchange.

The IA770 consists of license-file-activated software that resides on the S8300 Server, and an ICC daughter card, which is field-installable and upgradeable. For Communication Manager 2.2 and later, new installations will implement IA770 Embedded Messaging H.323 integration on the S8300, and will no longer use the ICC daughter card.

Voice Announcement over the LAN

Voice Announcement over the LAN (VAL) capabilities are co-resident on the Avaya G700 Media Gateway. This G700 VAL announcement capability allows backup and restore of announcements to an external PC or a file server on the customer's local area network (LAN), in addition to internal backup in Flash memory. The announcements are stored as industry-standard waveform (.wav) files. This enables customers to create high-quality, studio announcements, save the announcements to their PC or server, and then share the same announcements with multiple Avaya Application Solutions. Other features of the G700 VAL announcement offer include:

- A G700 VAL announcement source functions the same as the TN2501AP for administration, recording, file handling using FTP, playback, and measurements.
- Each G700 VAL announcement source used is counted as a VAL board towards the Maximum VAL boards on the customer-options screen. The S8300 Server now comes with a license entitlement for using up to 50 VAL circuit packs. The S8700-series Server comes with a license entitlement for one, and requires the purchase of additional licenses to enable the maximum of 50 which applies to both TN2501AP and G700 VAL sources.

- Voice quality is impacted when played over IP. However, quality is acceptable even with 2 hops and 10-msec delay.
- The use of G700 VAL sourced announcements impacts that gateway's overall occupancy, and IP Telephony resources (for example, high use global announcements such as the main greeting and some VOAs) should be handled by TN2501 circuit packs if the agents are not homed to that G700.
- FTP access for the G700 announcements use the same IP address as the address that is assigned to the G700 when installed (this address is displayed on the Media-Gateway form).

S8300 primary controller architecture

The S8300 Server has the same form factor as the Avaya media modules. The S8300 is installed in slot V1 of the G700, G450, G350, or G250 Media Gateway. The S8300 can be configured as either a primary controller (a.k.a. "ICC") or as a local survivable processor (LSP).

Configured as a primary controller, the S8300 provides Communication Manager call control. The controller targets the small-line-size, cost-conscious portion of the market, and as such, must be cost competitive with other solutions. The controller is based on standard Intel IA32 architecture, and runs the industry-standard Linux operating system.

The S8300 runs the following co-resident applications:

- H.248 Media Gateway Controller
- H.323 GateKeeper
- Communication Manager Feature Server
- INTUITY AUDIX Messaging system (installed in the G700)

The S8300 primary controller, when installed in the G700, can be ordered both with and without INTUITY AUDIX support.

The S8300 faceplate provides connectivity for two USB devices, and an Ethernet port for technician access. The faceplate also has operational LEDs and a shutdown switch. The media module backplane connector provides the interfaces for the internal 10/100 Ethernet bus and the TDM Bus.

For information on S8300 performance and capacities, see Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities on page 34.

S8300 as an LSP

The S8300 Server installed in a G700, G450, G350, or G250 Media Gateway can be configured as a Local Survivable Processor (LSP). The LSP provides survivability when the primary controller, either an S8300 ICC or an S8700-series External Communications Controller (ECC), is inaccessible. Each system can have multiple LSPs. Each LSP has a copy of the primary controller's translations. The translations are updated regularly from the primary controller by way of a virtual link through an IP network. Typically, all LSPs are in idle mode, where the LSPs are not processing any calls. When the Media Gateway's Processor (MGP) or individual IP endpoints perceive the primary controller to be unreachable, the MGP or the IP endpoints attempt to register with an LSP. The LSP does not actively take over when the primary controller becomes unreachable, but waits for MGPs and IP endpoints to register with it. Each LSP runs in license-normal mode until IP Telephones or MGPs register with it, which triggers the LSP to move into a license-error mode. Each LSP can run in active mode for a maximum of 10 days per outage before it must be reset manually.

Based on administration of Communication Manager, the G700/G450/G350/G250 LSP can return control of the G700/G450/G350/G250 Media Gateway to the primary controller (server) automatically when the connection is restored between the media gateway and the primary controller. By returning control of the media gateways to the primary controller automatically, Communication Manager software easily and quickly eliminates the fragmentation between remote gateways in the network created by LAN/WAN communication failures with the primary controller. The fall-back from the LSP to the primary controller may also be manual using a reset on the LSP. This reset breaks the communication between the LSP and each registered endpoint. This break causes the endpoints to register with the primary controller. However, most active calls are preserved.

Note:

The S8500 can also be configured as an LSP.

G450 Media Gateway

For additional information on the G450, see *Overview for the Avaya G450 Media Gateway*, 03-602058.

The Avaya G450 Media Gateway is a multipurpose media gateway that can be deployed in medium- to large-sized branch locations or in wiring closets servicing buildings and floors, in a campus environment. It works in conjunction with Avaya Communication Manager IP telephony software running on Avaya S8xxx Servers to deliver intelligent communications to enterprises of all sizes.

The G450 combines telephone exchange and data networking, by providing PSTN toll bypass and routing data and VoIP traffic over the WAN. The G450 features a VoIP engine, an optional WAN router, and Ethernet LAN connectivity. The G450 provides full support for Avaya IP and digital telephones, as well as analog devices such as modems, fax machines, and telephones.

The G450 can support up to 450 users when deployed as a branch gateway in a mid to large branch office of a large enterprise or a call center, and can serve up to 2400 users when deployed as a campus gateway. Both configurations require Avaya Communication Manager IP telephony software running on one or more Avaya S8xxx Servers. The 450 user capacity is reached when the Avaya S8300 server is used and the 2400 user capacity is reached when the Avaya S8500 Server is used.

Telephone services on a G450 are controlled by the Avaya S8700-series, S8500, and S8400 Servers as External Call Controllers (ECCs) over the LAN or WAN. The G450 also supports the Avaya S8300 Server operating either as an ECC or as an Internal Call Controller (ICC), with the S8300 embedded in the G450.

An S8300 ICC can be used in addition to an ECC with the S8300 installed in the G450 as a Local Survivable Processor (LSP) designed to take over call control in the event that the ECC fails or the WAN link between the branch office and main location breaks. The LSP provides full featured telephone service survivability for the branch office. The G450 itself also features Standard Local Survivability (SLS), which provides basic telephone services in the event that the connection with the primary ECC is lost.

The G450 is a scalable device with a basic configuration consisting of 1 power supply unit (PSU), 256 MB RAM, and a single DSP childboard supporting either 20 or 80 VoIP channels. This configuration can be enhanced by adding a redundant PSU, up to two RAM modules of 1 GB each, and up to three additional DSP childboards, increasing the number of VoIP channels to 240 channels.

G450 Features

G450 features include:

- Modular gateway features:
  - 9-slot chassis (one slot for main board and eight slots for media modules)
  - Swappable main board module
  - Hot swappable media modules
  - Support for two load sharing hot swappable power supply units
  - Hot swappable fan tray
  - VoIP DSPs (up to 240 channels)
  - Memory SIMMs
  - Contact Closure support
- Voice features:
  - H.248 gateway
  - Voice line interfaces: IP phones, Analog phones, Avaya DCP phones, BRI Phones, FXS/Fax, VoIP, Fax and modem over IP
  - Voice trunk interfaces: FXO, BRI, T1/E1

  - Supported CODECs: G.711A/µLaw, G.729a, G.726
  - DHCP and TFTP server to support IP phones images and configuration
  - Announcements and Music on Hold (MoH) support
- Survivability features for continuous voice services:
  - Local Survivable Processor (LSP, with S8300) — failover to LSP is connection-preserving
  - Standard Local Survivability (SLS)
  - Emergency Transfer Relay (ETR)
  - Modem Dial Backup
  - Dynamic Call Admission Control (CAC) for Fast Ethernet, Serial, and GRE tunnel interfaces
  - Inter-Gateway Alternate Routing (IGAR)
- Routing and WAN features:
  - Two WAN 10/100 Ethernet ports with traffic shaping capabilities
  - T1/E1 and USP interfaces
  - PPPoE, Frame-relay, and PPP
  - Routing Protocols: Static, OSPF, RIP
  - VRRP
  - Equal Cost Multi Path routing (ECMP)
  - IPSec VPN (requires license)
  - cRTP
  - WAN Quality of Service (QoS)
  - Policy-based routing
  - DHCP relay
  - GRE tunneling
  - Dynamic IP addressing (DHCP client/PPPoE)
  - Object tracking
  - Backup Interface
- Security hardened gateway features:
  - Media and signaling encryption
  - Secured management
  - Digitally signed gateway firmware
  - Managed security service support
  - Access list support

- Management features:
  - Avaya G450 Device Manager
  - Embedded Web Manager
  - RADIUS Authentication support
  - SNMPv1 traps and SNMPv3 notifications
  - Telnet and SSHv2 support
  - SCP, TFTP and FTP support
  - Syslog
  - Modem access for remote administration
  - Converged Network Analyzer (CNA) test plug
  - Packet Sniffing
  - RTP-MIB
  - Backup and Restore on Flash drive

G450 physical description

Figure 8: The Avaya G450 Media Gateway Chassis

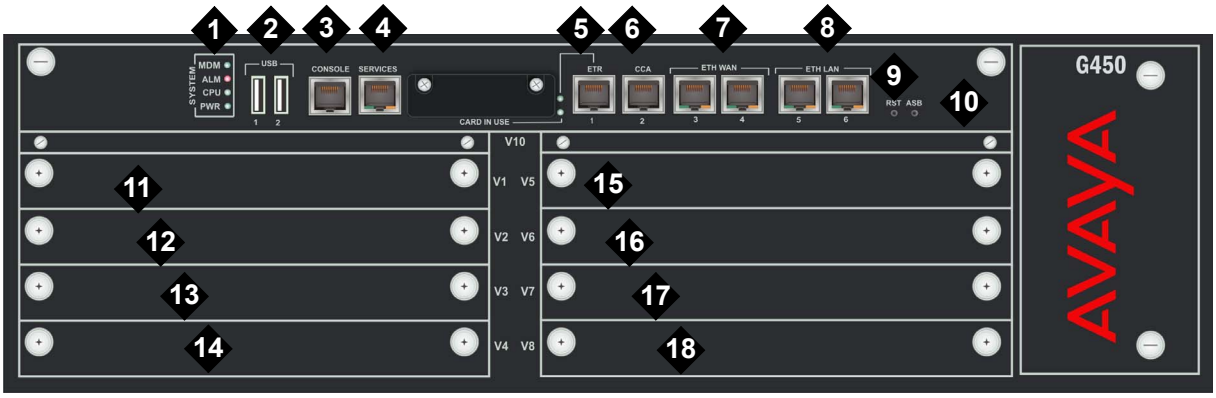


Figure notes:

1. System LEDs
2. USB ports
3. Console port
4. Services port
5. ETR (Emergency Transfer Relay) port
6. CCA (Contact Closure Adjunct) port
7. ETH WAN ports
8. ETH LAN ports
9. RST button
10. ASB button
11. V1 — slot for standard media module or S8300 Server
12. V2 — standard media module slot
13. V3 — standard media module slot
14. V4 — standard media module slot
15. V5 — standard media module slot
16. V6 — standard media module slot
17. V7 — standard media module slot
18. V8 — standard media module slot

The Avaya G450 Media Gateway is a versatile device with powerful capabilities. To implement the various services that are supported, a variety of swappable internal components called media modules are available.

Supported media modules in the G450

Table 5: Supported media modules

Media module	Description
S8300	CM server
Telephony media modules	
MM711	8 universal analog ports
MM714	4 analog telephone ports and 4 analog trunk ports

Table 5: Supported media modules (continued)

Media module	Description
MM716	24 analog ports
MM712	8 DCP telephone ports
MM717	24 DCP telephone ports
MM710	1 T1/E1 ISDN PRI trunk port
MM720	8 ISDN BRI trunk or endpoint (telephone or data) ports
MM722	2 ISDN BRI trunk ports
WAN media modules	
MM340	1 E1/T1 data WAN port
MM342	1 universal serial data WAN port

CAUTION:
The MM340 and MM342 are not supported by the Avaya G700 Media Gateway. Do not insert an MM340 or MM342 media module into an Avaya G700 Media Gateway.

Voice over IP (VoIP)

The G450 provides VoIP services over the LAN and WAN. The G450 supports up to four VoIP DSP childboards. Two types of childboard are supported, one providing 80 active VoIP channels and the other providing 20 active VoIP channels. The maximum number of active channels supported is 240. All channels can be bi-directional FAX, G.711 u/A, G.726A, or G.729A/AB calls.

Additional features

The G450 also provides the following voice-related features.

Call center capabilities

With large announcement storage, large voice trunk capacity, and 64 announcement ports for announcement record and playback, the G450 supports call center features.

Emergency Transfer Relay (ETR)

The Emergency Transfer Relay (ETR) feature provides basic telephone services in the event of a power outage or a failed connection to Avaya Communication Manager. The ETR supports the connection of two external 808A ETR panels. Each 808A Emergency Transfer Panel provides emergency trunk bypass or power-fail transfer for up to five incoming trunk loops to five analog phones and maintains connections on return from emergency transfer mode.

Contact closure

The contact closure feature is a controllable relay providing dry contacts for various applications. To implement the contact closure feature, connect an Avaya Partner Contact Closure Adjunct box to the CCA port on the G450 chassis. The adjunct box provides two contact closures that can be operated in either a “normally closed” or “normally open” state. The contact closures can control devices such as devices that automatically lock or unlock doors or voice recording units. The CCA port can be configured so that the connected devices can be controlled by an end device, such as a telephone. For example, a user can unlock a door by keying a sequence into a telephone keypad.

Fax, modem, TTY over IP

The G450 supports fax, modem, and TTY over IP.

LAN services

You can use the Avaya G450 Media Gateway as a LAN switch. You can also integrate the G450 into an existing LAN.

Physical media

The G450 provides LAN services through the fixed LAN ports on the chassis front panel for the connection of external LAN switches or local data devices. The LAN ports are connected to the internal LAN switch and support HP auto-MDIX, which automatically detects and corrects the polarity of crossed cables. This results in simplified LAN installation and maintenance.

VLANs

In the G450, you can configure VLANs on the fixed LAN ports.

The G450 supports up to 64 VLANs. The following VLAN features are supported:

- VLAN port grouping. Port VLANs can be used to group LAN ports into logical groups.
- Ingress VLAN Security. You configure a list of ingress VLANs on each port. Any packets tagged with an unlisted VLAN are dropped when received on the port.
- Class of Service (CoS) tagging. Packets are tagged with VLANs per CoS.
- Inter-VLAN routing. You can configure specific VLANs to permit access to the WAN while others can be configured to deny access to the WAN.

Rapid Spanning Tree Protocol (RSTP)

The IEEE 802.1D (STP) and IEEE 802.1w (RSTP) Spanning Tree Protocols are supported on the ETH LAN ports.

Port mirroring

The G450 supports network traffic monitoring by port mirroring. You can configure port mirroring on any LAN port. You implement port mirroring by connecting an external traffic probe device to one of the LAN ports. The probe device monitors traffic that is sent and received through other ports by copying the packets and sending them to the monitor port.

Port redundancy

You can configure port redundancy on the G450. Port redundancy allows you to provide both a primary link and a backup link to an important resource.

WAN services

The G450 has an internal router and provides direct access to outside WAN lines. You can use the G450 as the endpoint device for a WAN line. You can also use the G450 as the router for a WAN line with an external endpoint device.

Physical media

To use the G450 as the endpoint device for a WAN, install a WAN media module and connect the WAN line to a port on the media module. When you connect a WAN line to a media module, the G450 serves as the router for the WAN line.

You can also use the fixed ETH WAN Fast Ethernet port as a WAN endpoint by configuring the port's interface for PPPoE encapsulation (ADSL modem) or Ethernet-DHCP/static IP (cable modem).

To use the G450 as a router, connect the external endpoint device to the ETH WAN port on the G450 front panel using a standard network cable.

WAN line support

The G450 supports the following types of data WAN line:

- E1/T1
- Universal Serial Port
- PPPoE (ADSL modem)
- Ethernet-DHCP/static IP (cable modem)

Media modules necessary for each WAN line

The table below lists which media modules to install to connect each type of outside WAN line.

Table 6: Outside WAN lines supported and matching media modules

WAN line	Media modules
Universal Serial Port	MM342
E1/T1 data lines	MM340
PPPoE (ADSL modem)	Chassis
Ethernet (DHCP/static IP) (cable modem)	Chassis

Management access security features

The G450 features the following management security mechanisms:

- A basic authentication mechanism in which users are assigned passwords and privilege levels
- Support for user authentication provided by an external RADIUS server
- SNMPv3 user authentication
- Secure data transfer via SSH and SCP with user authentication
- ASG authentication for remote service logins. ASG is a challenge-response authentication method that is more secure than password authentication and does not require a static password.

Network security features

The Avaya G450 Media Gateway provides the following network security features:

- Private secure connections can be configured between the G450 and a remote peer, using VPN (Virtual Private Network). VPN at the IP level is deployed using a standards-based set of protocols defined by the IETF called IPSec. IPSec provides privacy, integrity, and authenticity to information transferred across IP networks.
- Protection against DoS (Denial of Service) attacks via:
  - MSS notifications. The G450 identifies predefined or custom-defined traffic patterns as suspected DoS attacks and generates SNMP notifications, referred to as Managed Security Services (MSS) notifications. MSS notifications are intercepted and, if certain conditions are met, may be forwarded to the Avaya Security Operations Center (SOC) as INADS alarms. The SOC is an Avaya service group that handles DoS alerts, responding as necessary to any DoS attack or related security issue.

- SYN cookies, which protect against a well-known TCP/IP attack in which a malicious attacker targets a vulnerable device and effectively prevents it from establishing new TCP connections.

Alarms and troubleshooting features

The G450 has extensive features for error detection, alarms, and troubleshooting. Detailed diagnostic information and troubleshooting are provided by software-based solutions accessible by laptop computers in the field or remotely from an administrator's computer. *Administration for the Avaya G450 Media Gateway*, 03-602055, provides a comprehensive guide to configuring and using these solutions.

Converged Network Analyzer (CNA) test plug

CNA test plugs are a component of CNA, a distributed system tool for real-time network monitoring that detects and diagnoses converged network-related issues. CNA is deployed in the media gateway to identify any network conditions or impairments that can degrade the user experience for IP telephony and to monitor overall network performance. Test plugs in media gateways provide the ability to measure end-to-end service to the edge of the PSTN, or at points where codec changes are required for interworking between high (LAN) and low (WAN) speed links.

Link Layer Discovery Protocol (LLDP)

LLDP simplifies network troubleshooting and enhances the ability of network management tools to discover and maintain accurate network topologies in multi-vendor environments. LLDP defines a set of advertisement messages (TLVs), a protocol for transmitting the TLVs, and a method for storing the information contained in the received TLVs. This allows stations attached to a LAN to advertise information about the system and about the station's point of attachment to the LAN to other stations attached to the same LAN. These can be reported to the management station via SNMP MIBs.

LLDP is supported on the front panel ETH LAN ports.

G250 and G350 Media Gateways

The Avaya G250 and G350 Media Gateways form part of Avaya Enterprise Connect, Avaya's solution for extending communication capabilities from the headquarters of an organization to all collaborative branch locations. Avaya Enterprise Connect helps you provide the same high quality services to all organization members, regardless of their location.

The G250 and G350 are high-performance converged telephony and networking devices that are located in small branch locations, providing all infrastructure needs in one box — telephone exchange and data networking. The G250 and G350 each feature a VoIP engine, WAN router, and Power-over-Ethernet (PoE) LAN switch. The G350 provides full support for legacy DCP and analog telephones. The G250 supports legacy analog telephones, but not DCP telephones.

The G350 is designed for use in a 16- to 24-user environment, but can support sites with up to 40 stations. The G250 media gateway is designed for smaller branch offices with two to eight users.

Telephone services on a G250/G350 are controlled by a Media Gateway Controller (MGC). You can use a server running Avaya Communication Manager call processing software as an MGC. Both the G250 and the G350 integrate seamlessly with Avaya Servers S8700-series, S8500, and S8300 to provide the same top quality telephony services to the small branch office as to the headquarters of the organization.

The MGC can be located at the headquarters and serve the G250/G350 remotely. The G250/G350 can optionally house an internal Avaya S8300 Server as a local survivable processor (LSP) or as the primary MGC for standalone deployment. When the primary MGC is located at a remote location, the G250 features Standard Local Survivability (SLS). SLS consists of a module built into the G250 itself to provide partial backup MGC functionality in the event that the connection with the primary MGC is lost. An additional option is Enhanced Local Survivability (ELS). ELS can be provided for both the G250 and the G350 by installing an S8300 Server as an LSP, capable of providing full MGC functionality in the event that the connection with the primary MGC is lost.

In addition to advanced and comprehensive telephony services, the G350 provides full data networking services, precluding the need for a WAN router or LAN switch.

The G350 is a modular device, adaptable to support different combinations of endpoint devices. Pluggable media modules provide interfaces for different types of telephones and trunks. A combination is selected to suit the needs of the branch. A LAN media module with PoE standard compliant Ethernet ports provides support for IP telephones as well as all other types of data devices. A range of telephony modules provides full support for legacy equipment such as analog and digital telephones.

The G250 supports the connection of PCs, LAN switches, IP phones, analog telephones, and trunks, using fixed analog and PoE ports on the chassis. A media module slot supports either of two WAN media modules, for connection to a WAN. The G250 is available in a special BRI model (G250-BRI). The G250-BRI replaces three out of four of the G250's fixed analog trunk ports with two ISDN BRI trunk ports.

G250 and G350 Features

G250 and G350 features include:

- Avaya Communication Manager server management
- Call center capabilities
- DHCP client, server, and relay functions
- Dynamic Call Admission Control (CAC) for Fast Ethernet, Serial, and GRE tunnel interfaces
- Dynamic IP addressing
- Extensive alarming and troubleshooting features

- Fax and modem over IP
- Frame-Relay
- GRE tunneling
- Inter-Gateway Alternate Routing (IGAR)
- MGC automatic switchover, migration, and survivability features
- Modem access for remote administration
- Modem backup connection to the MGC
- OSPF
- Policy-based routing
- Port mirroring
- Port redundancy (G350 only)
- Power-over-Ethernet LAN Switching
- PPP
- PPPoE
- RADIUS Authentication support
- RIP
- SNMP traps (v1 and v2 only) sent to the primary controller
- SNMP v3
- Spanning Tree Protocols IEEE 802.1D (STP) and IEEE 802.1w (RSTP) (G350 only)
- SSH Authentication support
- Support for traditional telephones and trunks
- Survivability features for continuous voice services
- VLANs
- VoIP Media Gateway services
- VPN support
- WAN Quality of Service (QoS)
- WAN routing and connectivity
- Weighted Fair Queuing (WFQ)

Modes of Deployment

The G250 and G350 can each be deployed in one of two basic working modes:

- Distributed Avaya Enterprise Connect.

  In this mode, the G250/G350 is controlled by an external MGC. This may be a standalone server, such as the S8500, S8700-series, or a separate media gateway in a standalone configuration. In systems with Enhanced Local Survivability (ELS), the G250/G350 also houses an S8300 Server module to function as a Local Survivable Processor (LSP), which can take over control of the G250/G350 if the external MGC stops serving the G250/G350.

- Standalone.

  In this mode, the G250/G350 is controlled by an internally housed S8300 Server module.

Multiple G250s and G350s may be deployed in many remote branches of a large organization. Large branches or main offices may deploy an Avaya G700 Media Gateway, which provides similar functionality to the G350 for a larger number of users. Up to 250 G250, G350, and G700 Media Gateways may be controlled by a single external S8700-series Server.

G350 Configurations

The G350 is a modular device with multiple configuration possibilities to meet specific individual needs. Six slots in the G350 chassis house various media modules, providing connections for different telephones, telephone trunks, data devices, and data lines.

Server configuration options for the G350 include:

- Standalone. In this configuration, one media module slot houses the S8300 internal Server, which runs the call control applications for the G350. The remaining slots house a customized selection of media modules, which connect to circuit-switched phones, trunks, and data devices. This configuration is capable of supporting up to 40 stations (maximum of 26 legacy Analog/DCP stations) and 35 trunks, including both circuit-switched and packet-switched (IP) endpoints.
- Media Gateway. In this configuration, there is no internal server. The G350 is dependent on a separate controller. This may be an external standalone server such as the S8500, S8700-series, or the S8300 Server housed in a separate media gateway. All six media module slots are available to house a customized selection of media modules.
- Survivable. In this configuration, an external server provides primary controlling service to the G350. The S8300 populates one of the module slots as a backup controller and functions in Local Survivable Processor (LSP) mode. If the external server stops serving the G350, the S8300 takes over the service. As for standalone configuration, the remaining slots house a customized selection of media modules.

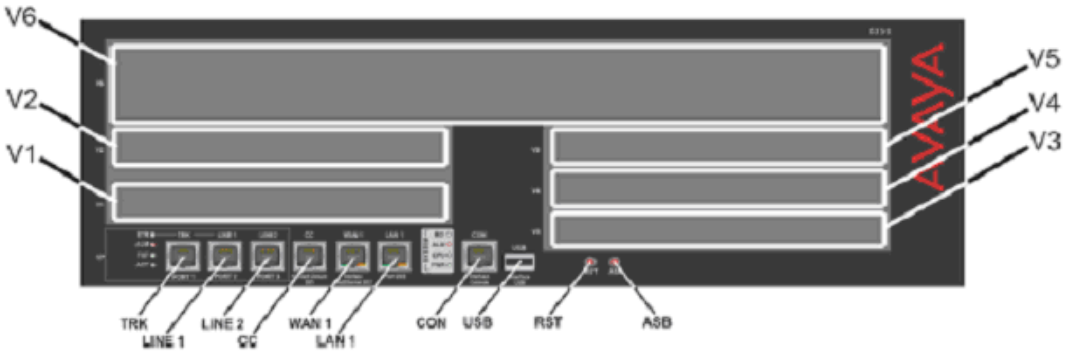
Each G350 should deploy as a single unit at a remote location. Multiple G350s may be deployed in many remote branches of a large organization. Large branches or main offices requiring more capacity than a single G350 should deploy one or more Avaya G700 Media Gateways. In addition to media gateway functions similar to those of G700, the G350 can optionally provide integrated power-over-Ethernet and WAN routing functions through media modules.

The G350 now supports up to 10 concurrent call center agents. Customers requiring more call center agents in a small branch office should consider the G700 media gateway.

G350 Specifications

The G350 chassis features six media module slots (V1 to V6) and various fixed ports and buttons. V1 to V5 are G700 form factor media module slots capable of housing existing G700 media modules. V6 is a high-density media module (HDMM) slot for housing new high capacity media modules (see Figure 9).

Figure 9: G350 chassis



The following tables describe the functions of the fixed ports and buttons on the G350 front panel.

Table 7: Fixed ports on the G350 front panel

Port	Description
TRK	An analog trunk port. Part of an integrated analog media module.
LINE 1, LINE2	Analog telephone ports of the integrated analog media module. An analog relay between TRK and LINE 1 provides Emergency Transfer Relay feature.
CC	RJ-45 port for ACS (308) contact closure adjunct box.
WAN 1	RJ-45 10/100 Base TX Ethernet WAN port.
LAN 1	RJ-45 10/100 Base TX Ethernet LAN switch port.
CON	Console port for direct connection of CLI console.
USB	USB port

Table 8: Buttons on the G350 front panel

Button	Description
RST	Reset button. Resets chassis configuration.
ASB	Alternate Software Bank button. Reboots the G350 with the software image in the non-default bank.

Table 9: Supported media modules for G350

Media module	Description
MM312 (HDMM)	24 DCP telephone ports
MM314 (HDMM)	24 10/100 Ethernet ports with Power over Ethernet and 1G Fiber port
MM316 (HDMM)	40 10/100 Ethernet ports with Power over Ethernet and 1G/ 10M/100M copper port.
MM340	1 E1/T1 WAN port
MM342	1 V.35/X.21 Universal Serial port (USP) WAN port
MM710	1 T1/E1 trunk port
MM711	8 universal analog ports
MM712	8 DCP telephone ports
MM714	4 analog telephone ports and 4 analog trunk ports
MM716	24 analog telephone ports
MM717	24 port DCP Media Module for G350/G700
MM720	8 ISDN BRI trunk ports
MM722	2 ISDN BRI trunk ports
(MM760)	Not supported for G350
S8300	Server (LSP)

The MM710, MM711, MM712, and MM720 are existing G700 media modules.

Table 10: Additional G350 functions and capacities

Function	Capacity
VoIP DSP engine	32 G.711 or 16 G.729 channels
Touch Tone Recognition (TTR)	15 channels
Announcement	6 playback, 1 record
Number of telephones	40 (18 analog)
Number of trunks (T1/E1)	40 (15 IP, 17 analog)
G700 form factor MMs	no more than three
MM710	no more than one
MM717 or MM712 (possibly with MM312)	no more than one
MM711 and/or MM714	no more than two
WAN modules (MM340 and MM342)	no more than two

G250 Configurations

Figure 10 shows the G250 Media Gateway chassis. Figure 11 shows the G250-BRI Media Gateway chassis.

Figure 10: The Avaya G250 analog Media Gateway Chassis,

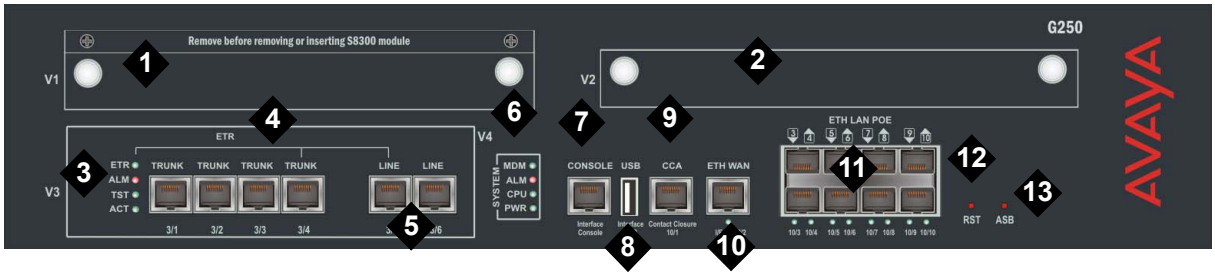


Figure notes:

1. **V1 — ICC/LSP Slot**
2. **V2 — WAN Media Module Slot**
3. **Analog port LEDs**
4. **Analog trunks**
5. **Analog line ports**
6. **System LEDs**
7. **Console port**
8. **USB port**
9. **Contact Closure (CCA) port**
10. **Ethernet WAN (ETH WAN) port**
11. **PoE LAN (ETH LAN PoE) ports**
12. **Reset (RST) button**
13. **Alternate Software Bank (ASB) button**

Figure 11: The Avaya G250 BRI Media Gateway Chassis,

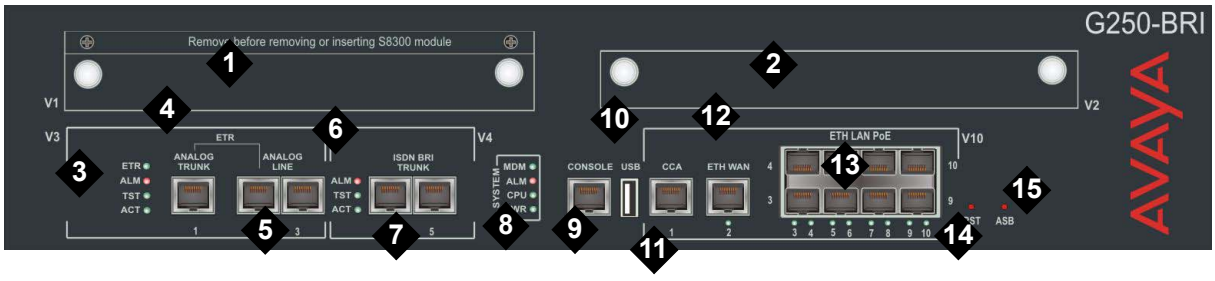


Figure notes:

1. **V1 — ICC/LSP Slot**
2. **V2 — WAN Media Module Slot**
3. **Analog port LEDs**
4. **Analog trunk**
5. **Analog line ports**
6. **ISDN BRI LEDs**
7. **ISDN BRI trunks**
8. **System LEDs**
9. **Console port**
10. **USB port**
11. **Contact Closure (CCA) port**
12. **Ethernet WAN (ETH WAN) port**
13. **PoE LAN (ETH LAN PoE) ports**
14. **Reset (RST) button**
15. **Alternate Software Bank (ASB) button**

Table 11: Fixed ports and buttons on the G250 front panel describes the functions of the fixed ports and buttons on the G250 front panel.

Table 11: Fixed ports and buttons on the G250 front panel

Port	Description
TRUNK	Four analog trunk ports (G250 analog Media Gateway) or one analog trunk port (G250-BRI Media Gateway).
LINE	Two analog telephone ports. An analog relay between TRUNK port 3/4 and LINE port 3/5 provides Emergency Transfer Relay (ETR) feature.
ISDN BRI TRUNK (G250-BRI Media Gateway)	Two 4 wire S/T ISDN BRI (Basic Rate Interface) 2B+D access ports with RJ-45 jacks. Each port interfaces to the central office at the ISDN T reference point. The ISDN BRI trunk ports do not support: • BRI stations • Combining both B channels together to form a 128-kbps channel
CONSOLE	Console RS-232 interface port for direct connection of CLI console. RJ-45 connector.
USB	USB port.
CCA	RJ-45 port for ACS (308) contact closure adjunct box.
ETH WAN	RJ-45 10/100 Base TX Ethernet port for connection to a cable or DSL broadband modem/router.
ETH LAN POE	Eight Power over Ethernet (PoE) LAN ports with 80 watts (aggregated for all ports) for connecting IP phones or any Ethernet devices, such as PCs.
RST	Reset button. Resets chassis configuration.
ASB	Alternate Software Bank button. Reboots the G250 with the software image in the alternate bank.

G250 DCP and G250 DS1 Media Gateways

Release 3.1 of Communication Manager introduces two new versions of the G250 Media Gateway.

The G250 DS1, supporting the T1/E1/PRI market, includes:

- One T1/E1/PRI trunk with fractional trunks allowed.
- One analog trunk with loop start only (no support for ground start or CAMA).
- Two analog lines and/or DID trunks (one with ETR).
- ETR.
- Eight Ethernet LAN PoE ports.
- 10/100 Ethernet WAN.
- One expansion slot for an ACM server module.
- One expansion slot for a data WAN media module.
- One console RS232 interface.
- One USB host interface.
- One contact closure relay control.

The G250 DCP includes:

- Four analog trunks Loop Start only (no support for Ground Start or CAMA)
- Two analog stations and/or DID trunks.
- Twelve DCP ports
- Two Ethernet LAN ports
- One 10/10 Ethernet WAN port
- One expansion slot for an ACM server module
- One expansion slot for a data WAN media module
- One console RS232 interface
- One USB host interface
- One contact closure relay control
- ETR

G150 Media Gateway

The G150 Media Gateway is a gateway aimed at small-office home office (SOHO) branch offices (1-8 users) of large enterprises, that seek all-in-one, centrally managed solution, hence

turning the SOHO branch into a seamless part of the enterprise's network. For information on the G150 Media Gateway, see *Hardware Description and Reference for Avaya Communication Manager*, 555-245-207.

IG550 Integrated Gateway

The IG550 Integrated Gateway is a part of Avaya's growing solutions for extending Communication Manager communication capabilities from the headquarters of an organization to all collaborative branch locations.The IG550 Integrated Gateway is an H.248 media gateway that combines Avaya's high-performance telephony and Voice over IP (VoIP) communications with the sophisticated routing capabilities of the Juniper J-Series routers.

The IG550 consists of the TGM550 Telephony Gateway Module (TGM550) and Telephony Interface Modules (TIMs). The IG550 is inserted into either a Juniper J4350 or J6350 Services Router. The IG550 is also connected over a LAN or WAN to an Avaya server running Communication Manager. Therefore, Avaya S8700-series, S8500, S8400, and S8300 Servers are able to provide the same top quality telephony services to the small branch office as to the headquarters of the organization. As a result, the IG550 provides full feature support for IP and analog telephones. See Figure 12.

Figure 12: Sample configuration of the IG550 in a Communication Manager network

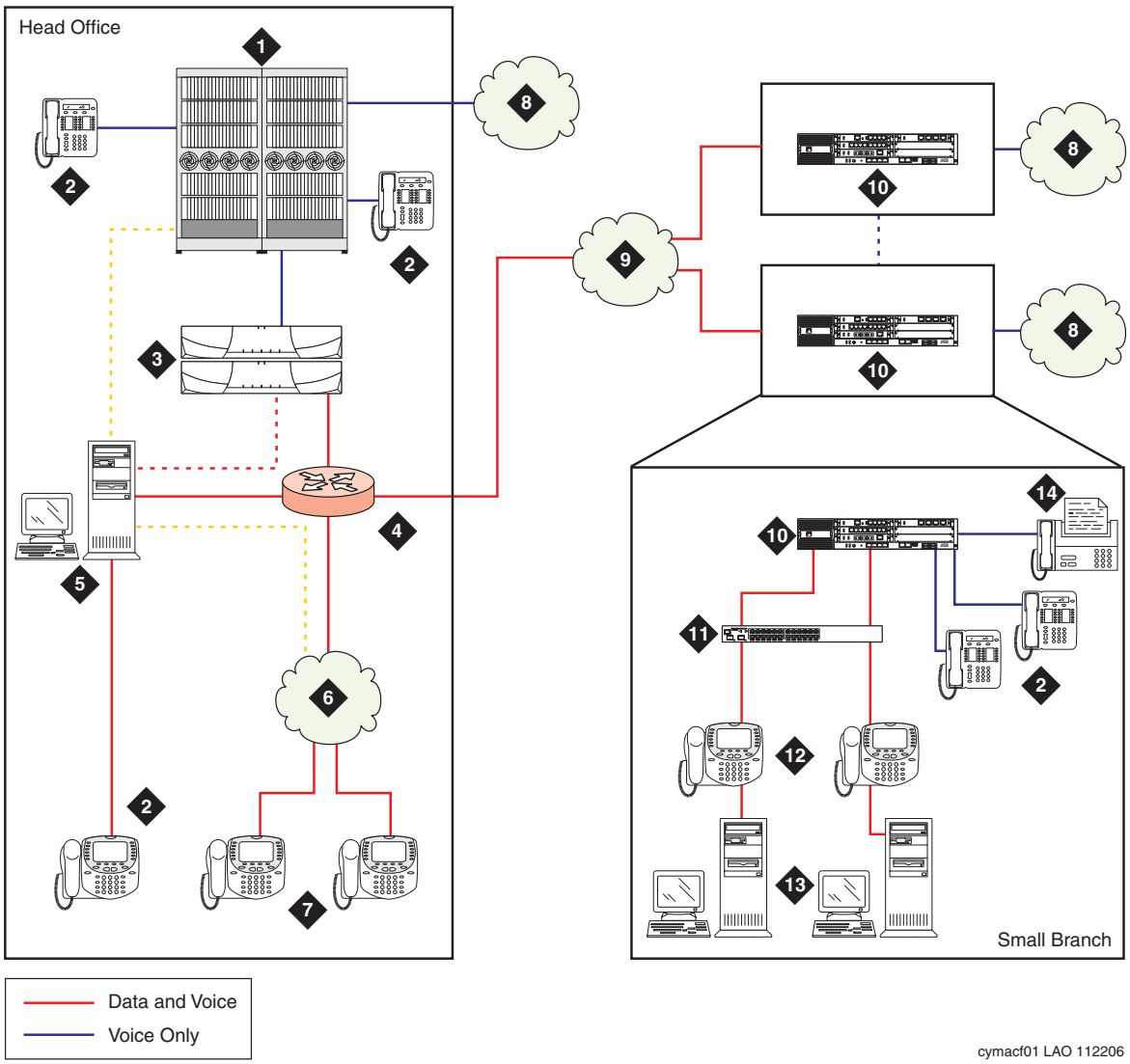


Figure notes: Sample configuration of the IG550 in a Communication Manager network

1. Media Gateway
2. Legacy telephones
3. S8700-series Server
4. Router
5. Integrated Management tools
6. LAN
7. IP telephones
8. Public Switched Telephone Network (PSTN)
9. WAN
10. J-series router with the IG550 Integrated Gateway
11. Ethernet switch
12. IP telephones
13. Personal computers
14. Fax

The IG550 is designed for use in a 20-to-100 user environment, with optimal performance at branch offices with 20 to 80 telephones.

The IG550 features Standard Local Survivability (SLS). SLS provides partial backup media gateway controller (MGC) functionality in the event that the connection with the primary MGC is lost.

In addition to advanced and comprehensive telephony services that are provided by the TGM550, the Juniper J-series Router, either the J4350 or J6350, provides full data networking services, precluding the need for a WAN router. The J-series routers use Juniper Physical Interface Modules (PIMs) for the hardware components to support network and routing features. The J-series routers also provide Ethernet connections to a separate Ethernet switch that IP phones connect to.

IG550 features

The IG550, through its use of the TGM550 and TIMS, supports the following features:

- Voice
  - Traditional telephones and trunks. In particular:
    - Two built-in line ports to support two analog telephones or incoming analog DID trunks on the TGM550
    - Two built-in analog trunk ports to support a trunk or trunks of the following types on the TGM550:
      - Loop start
      - Ground start
      - Analog Centralized Automated Message Accounting (CAMA)
      - Direct Inward/Outbound Dialing (DIOD) (Japan only)
    - An additional four analog line ports and four analog trunk ports on the TIM514
  - IP telephones
  - Survivability features for continuous voice services
  - VoIP Media Gateway services
  - ISDN-BRI trunks
  - E1/T1 DS1 trunks
  - Fax and modem over IP
  - Real Time Transport Protocol (RTP)/Real Time Transport Control Protocol (RTCP) processing
- Security
  - Remote Authentication Dial-in User Service (RADIUS) Authentication support

  - Simple Network Management Protocol (SNMP) traps and informs (v1 and v2 only) sent to the primary controller
  - SNMP v3 for remote management access, traps and informs
  - Secure Shell (SSH) Authentication support
  - Secrets encryption of configuration data
- Provisioning
  - Avaya Communication Manager server management
  - Integrated Management Solutions support
  - Extensive alarming and troubleshooting features
  - Modem access for remote administration
- Survivability
  - Media Gateway Controller (MGC) automatic switchover, migration, and survivability features
  - Modem backup connection to the MGC via a modem connected to the J-series router
  - Standard Local Survivability (SLS)
  - Dynamic Call Admission Control (CAC), in conjunction with the J-series router, for Fast Ethernet, Serial, and GRE tunnel interfaces
- Server and client applications
  - File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), and Secure Copy (SCP) client
  - Telnet client
  - FTP/TFTP server
  - Secure Shell (SSH) and Telnet server

For more detail on these features, see *Administration Guide and CLI Reference for the Avaya IG550 Integrated Gateway*, 03-601883.

J4350/J6350 Services Router features

The J4350 and J6350 Services Routers support the TGM550 and TIMS with the following features:

- WAN
  - Dynamic Call Admission Control (CAC) for Fast Ethernet, Serial, and GRE tunnel interfaces on the J-series routers
  - Routing protocols
    - Open Shortest Path First (OSPF)
    - Routing Information Protocol (RIP)

        - Border Gateway Protocol (BGP)
    - PPP over Ethernet (PPPoE)
    - Policy-based routing
    - Dynamic Host Configuration Protocol (DHCP) client, server, and relay functions
    - Generic Routing Encapsulation (GRE) tunneling
    - Dynamic IP addressing
    - Class of Service (COS)
    - Dynamic Name Server (DNS)
- LAN
    - Virtual LANs (VLANs)
- Security
    - Virtual Private Network (VPN) support
    - Network Address Translation (NAT)
- Provisioning
    - Modem access for remote administration
    - UNIX command line interface (CLI)
    - JUNOS software CLI
    - J-Web browser interface
- Survivability
    - Dynamic Call Admission Control (CAC) for Fast Ethernet, Serial, and GRE tunnel interfaces
    - VRRP
- Management applications
    - J-Web Quick Configuration
    - CLI

For detailed information on J-series router WAN and routing features and administration, see the following documents:

- *J4350 and J6350 Services Router Getting Started Guide*, Release 8.2
- *J-series Services Router Basic LAN and WAN Access Configuration Guide*, Release 8.2
- *J-series Services Router Advanced WAN Access Configuration Guide*, Release 8.2
- *J-series Services Router Administration, Release 8.2*

See the Juniper J-series router documentation at: http://juniper.net

IG550 and J4350 Services Router physical description

Figure 13: Example of the IG550 Integrated Gateway in a J4350 Services Router

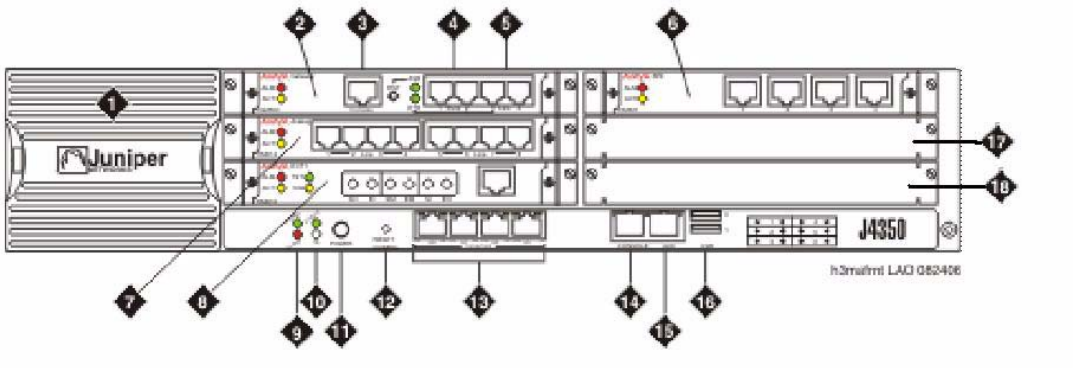
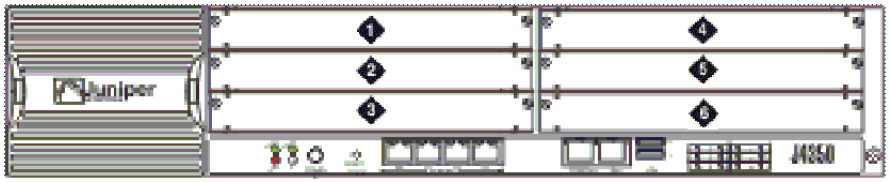


Figure notes:

1. **Juniper Services Router, J4350 shown**
2. **TGM550 Telephony Gateway Module (in slot V1)**
3. **TGM550 console port**
4. **TGM550 analog trunk ports**
5. **TGM550 analog line ports**
6. **TIM521 BRI telephony interface module (in slot V4)**
7. **TIM514 analog telephony interface module (in slot V2)**
8. **TIM510 E1/T1 telephony interface module (in slot V3)**
9. **J-series Router Alarm LEDs**
10. **J-series Router Power LEDs**
11. **Power button**
12. **Reset button**
13. **Gigabit Ethernet ports**
14. **Console port**
15. **Aux port**
16. **USB ports**
17. **Slot V5 (empty in illustration)**
18. **Slot V6 (empty in illustration)**

Slot locations on J4350 Services Router - The slots on the J4350 Services Router are identified as follows:

Figure 14: Slot numbers on the Juniper J4350 Services Router



The J-series router chassis has six slots. The TGM550 can be housed in any of the six router slots. The TIMs can also be housed in any slot. Gigabit Ethernet and Fast Ethernet PIMs can be housed only in slots 3 or 6. Other optional PIMs can be housed in any slots.

IG550 and J6350 Services Router physical description

Figure 15: The IG550 Integrated Gateway in a J6350 Services Router

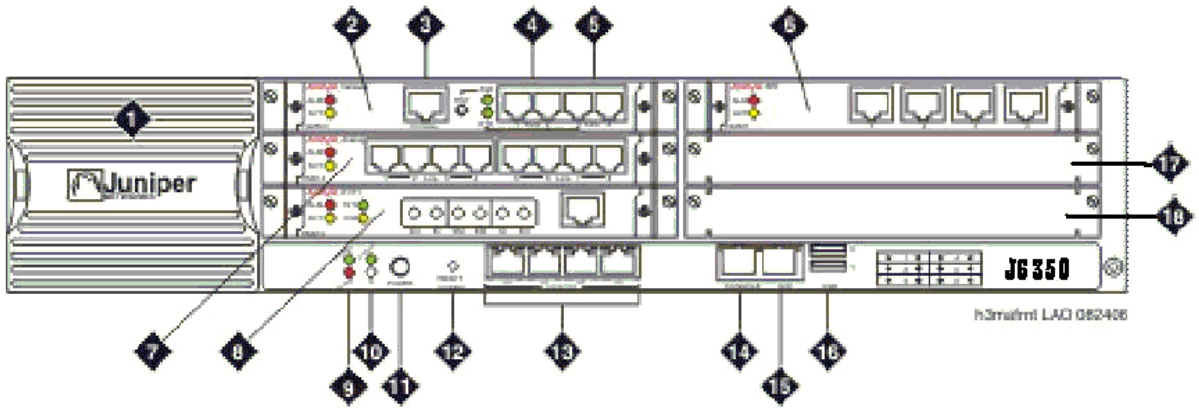


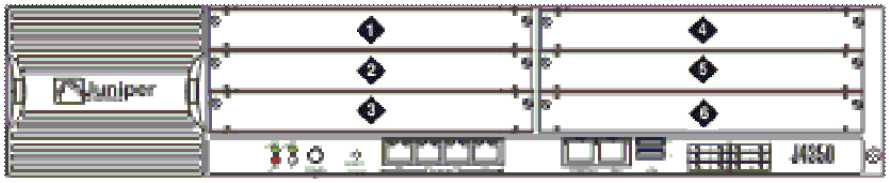
Figure notes:

1. Juniper Services Router, J6350 shown
2. TGM550 Telephone Gateway Module (in slot V1)
3. TGM550 console port
4. TGM550 analog trunk ports
5. TGM550 analog line ports
6. TIM521 BRI telephony interface module (in slot V2)
7. TIM514 analog telephony interface module (in slot V2)
8. TIM510 E1/T1 telephony interface module (in slot V4)
9. J-series Router Alarm LEDs
10. J-series Router Power LEDs
11. Power button
12. Reset button
13. Gigabit Ethernet ports
14. Console port
15. Aux port
16. USB ports
17. Slot V5 (empty)
18. Slot V6 (empty)

Slot locations on J6350 Services Router

The slots on the J6350 Services Router are identified as follows:

Figure 16: Slot numbers on the Juniper J6350 Services Router



The J-series router chassis has six slots. The TGM550 can be housed in any of the six router slots. The TIMs can also be housed in any slot. Gigabit Ethernet and Fast Ethernet PIMs can be housed only in slots 2, 3, 5, or 6. Other optional PIMs can be housed in any slots.

TGM550 physical description

Figure 17: The TGM550 Gateway Module

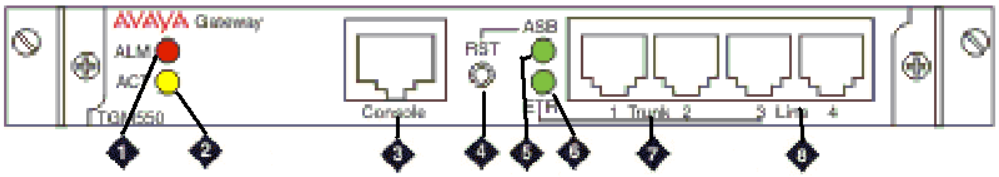


Figure notes:

1. Alarm LED
2. ACT LED
3. Console port
4. RST button
5. ASB LED
6. ETR LED
7. Analog trunk ports
8. Analog line ports

Supported optional modules in the J-series routers and the IG550

The IG550 Gateway Module supports a variety of optional internal boards called Telephony Interface Modules (TIMs). In addition, the Juniper J-series Routers support swappable internal components called Physical Interface Modules (PIMs).

Note:

This list of PIMs for J-series routers is a sample only. For a complete list of PIMs, see the Juniper J-series router documentation at http://juniper.net.

Table 12: Supported interface modules

Modules	Description
Telephony Interface Modules	
TIM514	4 analog telephone ports and 4 analog trunk ports
TIM510	1 E1/T1 trunk port, a DS1 level port that provides a wide variety of E1 or T1 circuit support. Can provide up to 30 E1 or 24 T1 channels

1 of 2

Table 12: Supported interface modules (continued)

Modules	Description
TIM521	4 ISDN BRI trunk ports providing up to 8 bearer channels
J-series Router Physical Interface Modules	
Dual-Port Serial PIM	2 Fast Ethernet ports and two serial ports
Dual-Port T1 or E1 PIM	2 Fast Ethernet ports and two E1/T1 ports, each providing up to 30 E1 or 24 T1 data channels for WAN connections
Dual-Port Channelized T1 or E1 PIM	2 T1 or E1 ports
T3 or E3 PIM	1 E3/T3 port for WAN connections
Gigabit Ethernet SFP ePIM	One Gigabit port
Gigabit Ethernet copper ePIM	One Gigabit port
Dual-Port Fast Ethernet PIM	2 Fast Ethernet ports
Four-Port Fast Ethernet ePIM	4 Fast Ethernet ports
4-Port ISDN BRI S/T PIM	4 ISDN BRI data-only ports
4-Port ISDN BRI U PIM	4 ISDN BRI data-only ports
ADSL PIM (Annex A)	1 port for DSL over an analog trunk
ADSL PIM (Annex B)	One port for ADSL over ISDN providing up to 32 virtual channels
G.SHDSL PIM	Two ports for 32 virtual channels of ATM over SHDSL connections
	2 of 2

Table 13 shows capacities of the supported interface modules.

Table 13: Interface module capacities

Description	Capacity	Comments
Servers registered as Media Gateway Controllers. If an MGC becomes unavailable, the IG550 uses the next MGC on the list.	4	The built-in SLS module can be considered a fifth MGC, although its functionality is more limited than that of a full scale server.
Module slots for TGM550,TIMs and PIMs	6	The J-series router allows any slot to be used for the TGM550 and any TIMs or PIMs.
Fixed analog line ports	2	
Fixed analog trunk ports	2	
Maximum number of TIMs	4	Up to 4 TIMs can be inserted into a J-series router.
Maximum number of TIM510 E1/ T1 TIMs	2	
Maximum number of TIM521 BRI TIMs	2	

CAUTION:
Some capacities may change. For the most up-to-date list, see *System Capacities Table for Avaya Communication Manager on Avaya Servers*, 03-300511.

Summary of services

The IG550 offers various services, a few of which are described below. For a complete description of services, see *Overview for the Avaya IG550 Integrated Gateway,* 03-60158.

Voice over IP (VoIP)

The IG550 features a VoIP engine that provides voice services over IP data networks. The IG550 allows you to use many types of telephones and trunks that do not directly support VoIP. The media gateway translates voice and signalling data between VoIP and the system used by the telephones and trunks, as follows: Avaya TIMs convert the voice path of traditional circuits such as analog trunk, and T1/E1 to a TDM bus inside the media gateway. The VoIP engine then converts the voice path from the TDM bus to a compressed or uncompressed and packetized VoIP on an Ethernet connection.

The G250 provides VoIP services over the LAN and WAN. The G250 supports the G.711, G.729A, G.729AB, and the G.726A codecs, for up to 80 concurrent calls.

Configuring media gateway options

The media gateway provides the following configuration options to help you ensure continuous telephone services:

- You can configure the media gateway to use up to four servers. If the MGC is an S8700-series server, the first server on the list will normally be the primary C-LAN board connected to the server. If the MGC is an S8400 or S8500, the first server on the list will be either the primary C-LAN board connected to the server or an Ethernet port on the server that has been enabled for processor Ethernet connections. If the MGC is an S8300, the first server on the list will be the IP address of the S8300. The remaining servers will be alternate C-LAN boards connected to the server (S8400, S8500, or S8700-series Servers), an S8300 configured as an Local Survivable Processor (LSP), or the port enabled as the Ethernet processor port on an S8500 configured as an LSP. In addition, the gateway can also register to the Standard Local Survivability engine (see the SLS description that follows).
- Using the connection preserving migration feature, you can configure the media gateway to preserve the bearer paths of stable calls in the event that the media gateway migrates to another MGC (including an LSP), including migration back from an LSP to the primary MGC. A call for which the talk path between parties in the call has been established is considered stable. A call consisting of a user listening to announcements or music is not considered stable and is not preserved. Any change of state in the call prevents the call from being preserved. For example, putting a call on hold during MGC migration will cause the call to be dropped. Special features, such as conference and transfer, are not available on preserved calls. Connection preserving migration preserves all types of bearer connects except BRI. PRI trunk connections are preserved.
- You can configure Standard Local Survivability (SLS) to enable a local media gateway to provide a degree of MGC functionality when no link is available to an external MGC. SLS is configured on a system-wide basis using the Provisioning and Installation Manager (PIM). Alternatively, SLS can be configured from the individual media gateway itself using the CLI. SLS supports all analog interfaces, ISDN BRI/PRI trunk interfaces, non-ISDN digital DS1 trunk interfaces, IP phone, and IP Softphone.

- You can configure the dialer interface to connect to the media gateway's primary MGC via a modem connected to the J-series router in the event that the connection between the media gateway and the MGC is lost.
- You can configure the Avaya Communication Manager to support the auto fallback feature, which enables a media gateway being serviced by an LSP to return to its primary MGC automatically when the connection is restored between the media gateway and the MGC. When the media gateway is being served by its LSP, it automatically attempts to register with its MGC at periodic intervals. The MGC can deny registration in cases in which it is overwhelmed with call processing, or in other configurable circumstances. By migrating the media gateway to the MGC automatically, a fragmented network can be unified more quickly, without the need for human intervention.

  Note:

  Auto fallback does not include survivability. Therefore, there is a short period during registration with the MGC during which calls are dropped and service is not available. This problem can be minimized using the connection preserving migration feature.
- The media gateway features a dynamic trap manager, which enables you to ensure that the media gateway sends traps directly to the currently active MGC. If the MGC fails, the dynamic trap manager ensures that traps are sent to the backup MGC.

Backup and restore

The IG550 allows the backup and restore of TGM50 data to an FTP server on the network.

You should backup TGM550 configuration data separately from the J-series configuration data.

You can backup J-series router data to a USB stick, the internal compact flash, or an external compact flash.

Converged Network Analyzer (CNA) test plug

CNA test plugs are a component of CNA, a distributed system tool for real-time network monitoring that detects and diagnoses converged network-related issues. CNA is deployed in the media gateway to identify any network conditions or impairments that can degrade the user experience for IP telephony and to monitor overall network performance. Test plugs in media gateways provide the ability to measure end-to-end service to the edge of the PSTN, or at points where codec changes are required for interworking between high (LAN) and low (WAN) speed links.

IG550 maximum media gateway capacities

Table 14: IG550 media gateway capacities

Description	Capacity	Comments
Busy Hour Call rate (BHCC)	800	
Maximum number of TGM550s controlled by an S8500 or S8700-series Server	250	This number also applies if a combination of Avaya G700 Media Gateways, Avaya G250 Media Gateways, and G350 Media Gateways are controlled by the same server.
Maximum number of TGM550s controlled by an S8400 Server	5	This number also applies if a combination of Avaya G700 Media Gateways, Avaya G250 Media Gateways, and G350 Media Gateways are controlled by the same server.
Maximum number of TGM550s controlled by an S8300 Server in a G350 or G700	49	This capacity is 50 if a combination of Avaya G700 Media Gateways, Avaya G250 Media Gateways, and G350 Media Gateways are also controlled by the same server. The S8300 must reside in a G700 or G350. Therefore, the maximum of 50 H.248 gateways supported by the S8300 means that only 49 of the 50 could be IG550s.
Servers registered as Media Gateway Controllers. If an MGC becomes unavailable, the IG550 uses the next MGC on the list.	4	The built-in SLS module can be considered a fifth MGC, although its functionality is more limited than that of a full scale server.
Maximum total number of telephones supported by the IG550	100	Maximum includes a combination of analog and IP telephones

CAUTION:

Some capacities may change. For the most up-to-date list, see *System Capacities Table for Avaya Communication Manager on Avaya Servers*, 03-300511.

For more information on the IG550 Integrated Gateway, see *Overview for the Avaya IG550 Integrated Gateway,* 03-60158.

Avaya S8400 Server

The S8400 Server is a Linux-based server that occupies a single slot in a standard TN carrier. The S8400 Server provides Communication Manager processing functionality in stand alone, single port network (PN), telephony systems supporting up to 900 stations.

The S8400 Server is composed of the:

- TN8400AP Server circuit pack
- TN8412AP S8400 IP Interface (SIPI) circuit pack

Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities on page 34 summarizes the capacity specifications of the Avaya S8400 Server.

TN8400AP circuit pack (S8400 Server) on page 76 shows the TN8400AP circuit pack.

Figure 18: TN8400AP circuit pack (S8400 Server)

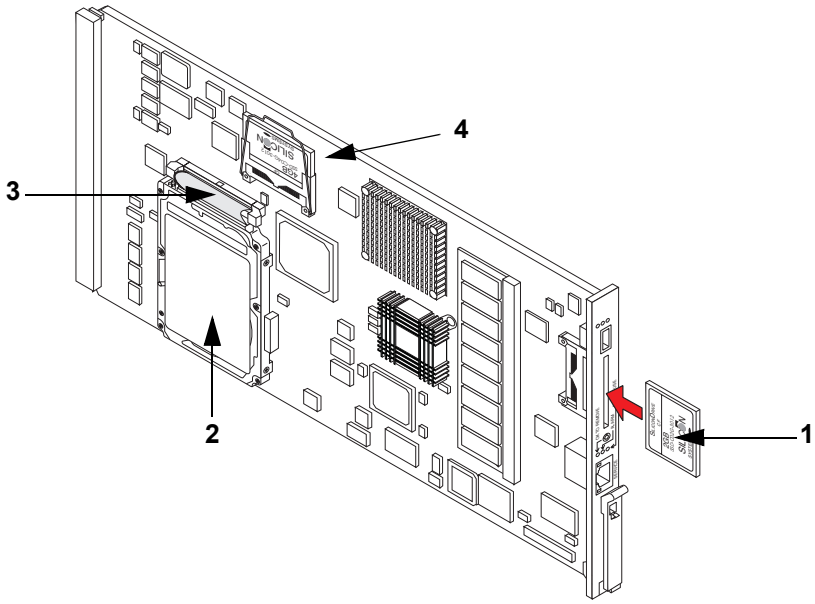


Figure notes:

1. **Compact flash**
2. **Hard disk drive**
3. **Ribbon cable to hard disk drive**
4. **Solid state drive**

The S8400 Server can replace the following platforms:

- DEFINITY CSI
- DEFINITY One/S8100
- IP600/S8100

For new installations, the PNs use the G650 Media Gateways. For migrations of current installations, use the S8400 Server as an upgrade path for current PNs based on G650 and G600 Media Gateways and CMC carriers. Since the S8400 Server supports only one port network, and different media gateways cannot be mixed in the same port network, a G650 Media Gateway cannot be added to an S8400 system that carries forward a CMC1 or G600 Media Gateway as a result of a migration.

The S8400 Server uses the TN8412AP S8400 IP Interface (SIPI) or the TN2312BP Internet Protocol Server Interface (IPSI-2) circuit pack to provide:

- circuit pack control within its port network
- cabinet maintenance
- tone-clocks
- emergency transfer switch functionality
- customer/external alarms.

The TN799DP Control-LAN (C-LAN) circuit pack provides firmware download functionality while the TN2501 Voice Announcement over LAN (VAL) circuit pack provides announcement functionality.

The S8400 Server provides a Voice over Internet Protocol (VoIP) based integrated messaging capability for up to 450 light duty users. This option requires that 8 ports of VoIP resources be provisioned with the S8400 Server. The hard disk drive stores the messages and a TN2302AP IP Media Processor circuit pack usually provides the VoIP resources.

An external messaging system is required when an S8400 Server based system is configured for more than 450 light duty users that requires messaging.

The S8400 Server supports a single port network (PN), which can be composed of:

- up to 5 G650s
- up to 4 CMC1s
- up to 3 G600s

The S8400 also supports up to 5 H.248 media gateways, including:

- G700
- G450
- G350
- G250

The S8400 can support up to 80 G150 Media Gateways.

The S8400 Server cannot be configured as an Enterprise Survivable Server (ESS) or Local Survivable Processor (LSP). But a G700, G450, G350, or G250 Media Gateway connected to an S8400 Server can have an LSP installed. In the event that the media gateway can no longer communicate with the S8400, the LSP takes over all call processing functions for that gateway. However, the LSP does not take on any of the call processing functions for those trunks and endpoints that are directly connected to the S8400.

The S8400 Server consists of three separate TN circuit packs; two required and one optional:

- TN8400AP circuit pack that provides
  - Avaya Communication Manager call processing
  - coresident voicemail
  - on board diagnostics
  - autonomous alarming
- TN8412AP S8400 IP Interface (SIPI) that provides
  - low-level control functions and services for a TN port network
  - tone detection and generation
  - carrier maintenance and diagnostics
  - input/output of alarm leads

  - emergency transfer
- An optional TN2302AP IP Media Processor if you run the optional embedded messaging (IA770) or run IP telephones. When running IP telephones, the TN2302AP interfaces between the Time Division Multiplex (TDM) bus and the IP network.

The S8400 Server uses a solid state drive and a hard disk drive to:

- run Avaya Communication Manager
- hold translations
- function as the primary storage device

The solid state drive and CD/DVD-ROM drive each can be configured as a bootable device. The boot sequence is as follows:

1. USB CD/DVD-ROM drive when you install it
2. Solid state drive

Communication between the S8400 and the TN8412AP is by IP link. The S8400 has an Ethernet NIC for the TN8412AP control link. You can connect this link by an external switch or point-to-point by a single Ethernet crossover cable. The TN8412AP has a single Ethernet interface for control.

The optional IA770 integrated messaging supports the equivalent of 8 ports of voice messaging simultaneously, and up to 450 light duty users. An external messaging system if more than 450 users are required or where the 450 users are "exceptionally heavy users." The exceptionally heavy users are defined as users who require more than 4.5 disk minutes/user/day or 10 port minutes/user/day. The following items are optional for all S8400 controlled systems:

- A TN799DP Control-LAN (C-LAN) circuit pack for the firmware download
- A TN2302AP IP Media Processor circuit pack might be needed to provide conversion between TDM and IP for all IP-based voice mail solution (IA770) and IP telephony. Up to 8 ports of the TN2302AP can be utilized by the IA770 integrated messaging option and the remaining ports may be used to support IP telephony systems.
- The S8400 generally uses the IA770 voice mail product that is an all IP solution and co-resides on the circuit pack. IA770 is a VoIP based integrated messaging option that requires up to 8 ports of VoIP resources.
- Customers provide an Ethernet switch if it is required.
- A TN771 Maintenance/Test circuit pack when:
  - There are 3 or more G650, G600, or CMC1 cabinets (G150 and H.248 gateways should not be included in this count) in the S8400 system, and
  - There are IP or ISDN endpoints (BRI and PRI trunks and BRI stations)

Mid-market to large enterprise

S8500 Server

The Avaya S8500 Server Platform is a simplex Linux-based server running Avaya Communication Manager software that replaces the DEFINITY SI and R processing platforms for small sites and for customers who do not require a duplicated server complex.

The S8500 supports all of the Avaya media gateways. The S8500 has the capacity to support up to 64 IP-connected port networks. Up to 3 MCC1 port networks can be directly connected. The S8500 can be configured as a primary controller, a Local Survivable Processor (LSP), or as an Enterprise Survivable Server (ESS).

The S8500 Server allows for a seamless migration from DEFINITY SI and R platforms. However, the S8500 will not support traditional circuit-switched Center Stage Switch or ATM Port Network Connectivity.

S8500 capacities

Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities on page 34 summarizes the performance and capacity specifications of the Avaya S8500 Server.

Avaya S8700-series Server, fiber-PNC configuration

The S8700-series Server with an MCC1 or SCC1 Media Gateway is targeted at Avaya's largest customers. These customers are typically experiencing rapid growth, and looking for ways to consolidate their network. These are customers who require high-end applications such as DEFINITY Call Center Solutions, CTI applications, Unified Messaging, multimedia conferencing, and voice/data network integration, and are evolving to an IP-intensive environment. This solution supports up to 44,000 telephones.

This solution is also targeted at smaller customers who made an investment in DEFINITY, and are looking for a smooth transition into industry-standard processors that will enable expanded communications capabilities.

The S8700-series Server is a large-office solution with the server in the headquarter locations and optional servers/gateways in the branch offices. The option of duplicated headquarters with branch and remote offices is also available.

For information on S8700-series Server performance and capacities, see Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities on page 34.

Because the inter port network TDM traffic flow is supported by a Center Stage Switch (CSS) or an Asynchronous Transfer Mode (ATM) switch using fiber-optic cables, this configuration is called *fiber-PNC*. The call control traffic between the server and the gateways is usually, but not necessarily, over a private dedicated Ethernet network that is provided by Avaya.

This solution is scalable to up to 44 port networks (PNs) through CSS configuration, and up to 64 PNs in an ATM configuration. The fiber-PNC solution has three reliability options:

- **Standard**. Duplicated S8700-series Servers with memory shadowing, two uninterruptible power supplies (UPS), one Layer-2 Ethernet switch, and one IPSI in each IPSI-connected PN.
- **High**. Standard reliability, plus a second Layer-2 Ethernet switch and a second IPSI in each IPSI-connected PN. This design provides for a second redundant call control network.
- **Critical**. High reliability plus duplication of the bearer network.

S8720 and S8730 Servers

The Avaya S8720 and S8730 Server Platforms are high-performance servers with AMD Opteron processors running Avaya Communication Manager software. The S8720 is a replacement server for the S8700 and S8710 Servers and the S8730 is a replacement for the S8720 Server. The S8720 and S8730 support a software duplication option that eliminates the need for the DAJ1 and DAL1 or DAL2 hardware-assist duplication cards.

The S8720 and S8730 systems support the Avaya MCC1, SCC1, CMC1, and G650 Media Gateways. The Avaya G700, G450, G350, G250, and G150 Media Gateways are also supported if there is a TCP/IP connection between the media gateway and a C-LAN circuit pack located in a MCC1, SCC1, CMC1, or G650 Media Gateway. The S8720 and S8730 have the capacity to support up to 64 port networks.

The S8720 Server is available in two configurations:

- Standard configuration.
- Extra large configuration that provides higher capacities.

The S8730 Server is available in a single extra large configuration with 4 GB of RAM and RAID controllers and an optional duplicated hard disk.

S8700-series Servers

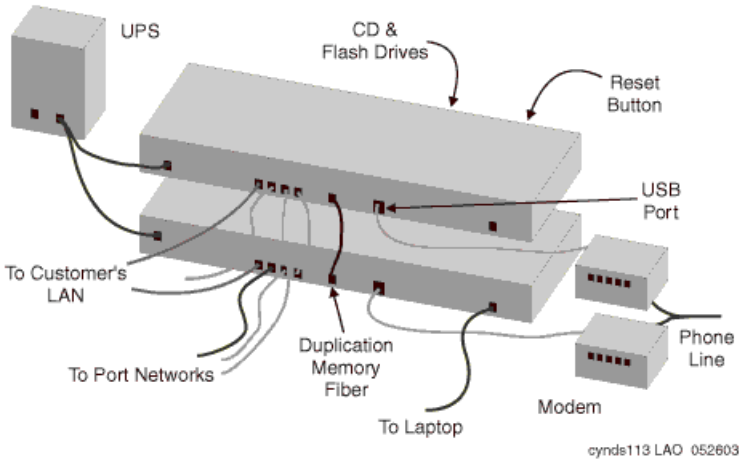
Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities on page 34 summarizes the performance and capacity specifications of the Avaya S8700-series Servers.

The Avaya S8700-series Server platform always consists of two servers running on a Linux operating system. In S8700-series fiber-PNC and IP-PNC configurations, the S8700-series Server provides the main feature and management processing capabilities of the system. The server is connected to other system and external components primarily through IP networks.

S8700-series external features

- Six 10/100 Ethernet NICs per server, which are used as follows:
  - Dual control network connections
  - A memory duplication link to the duplicated server
  - Administrative access from the corporate network
  - Technician access
  - One unused
- A PCMCIA Flash disk for translations backup
- USB ports for remote access connections (modems and other auxiliary devices)
- A reset button
- Support for global power
- A fiber-channel interface to support server duplication (except for S8720, S8730 software duplication)

Figure 19: Avaya S8700-series external features



UPS or power backup - The S8700-series Servers always require power backup to avoid power problems, and to ensure graceful shutdown of the system processes if the power fails. The AS1 700-VA UPS provides approximately 30 minutes of power backup. Combinations of battery extension modules and a 1500-VA UPS provide up to 8 hours of power backup.

The AS1 UPS units use SNMP traps to send an alarm when power fails. This action initiates a graceful shutdown process of the Linux server, including the call processing software.

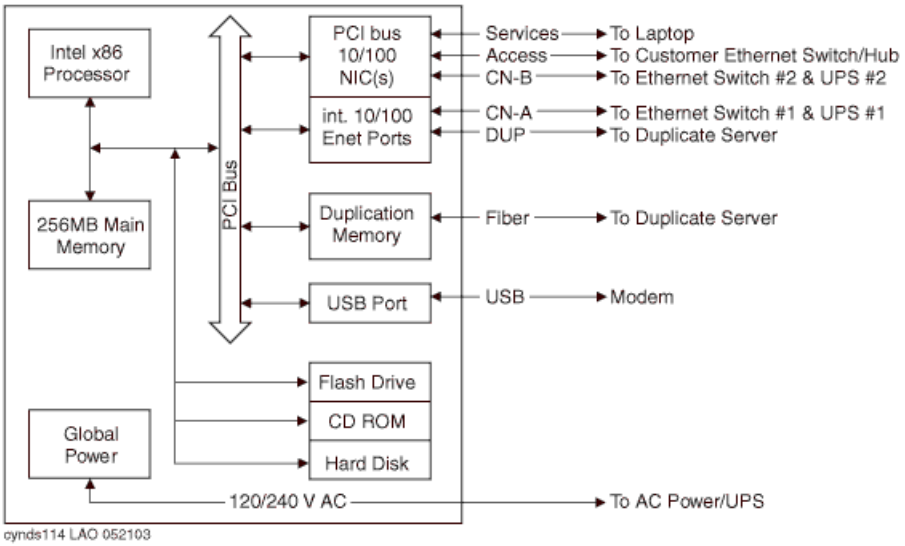
USB modem - Each S8700-series Server supports a Universal Serial Bus (USB) modem. For customers with an Avaya service contract, the modem is used to send alarms to the Avaya Services organization, and to facilitate maintenance by Avaya Services personnel.

Internal hardware elements

The server has the following specifications:

- 512 MB (S8710) or 1 GB (S8720) or 4 GB (S8730) of main memory
- SCSI hard disk for booting Linux and Communication Manager
- Combo DVD/CD-ROM drive for software installations and upgrades
- 2 (S8710) or 3 (S8720, S8730) USB ports
- USB Compact Flash card support

Figure 20: Avaya S8700-series Server schematic

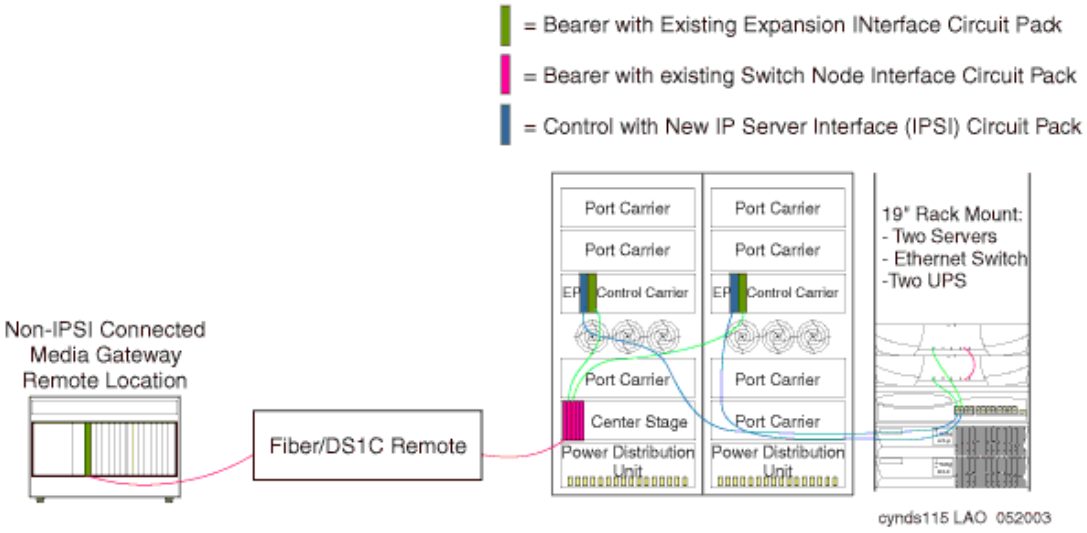


Other components

The S8700 in a fiber-PNC solution also includes the following components:

- L2/L3 data network switch or Ethernet switch with duplication option
- One or more IP Server Interface (IPSI) circuit packs (TN2312BP)
- A Center Stage Switch (CSS) or an ATM Switch for bearer connectivity
- One or more MCC1 or SCC1 Media Gateways, also known as port networks (PNs)

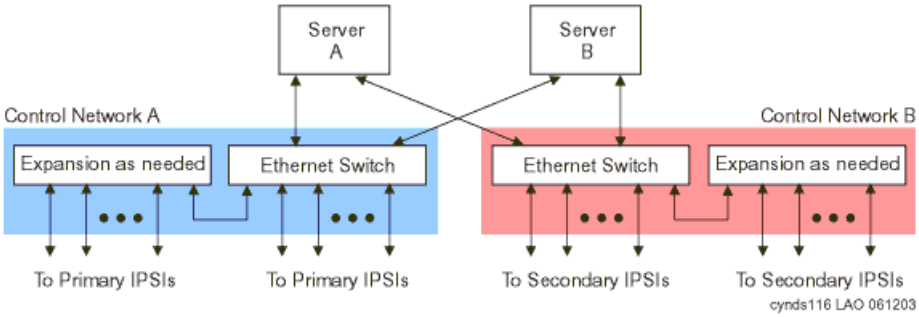
Figure 21: Avaya S8700/MCC1 fiber-PNC major components



Control network through an Avaya Ethernet switch

When designing S8700-series fiber-PNC systems, a control network connects the servers to the IPSIs through a 10/100 BaseT Ethernet. It consists of two separate Ethernet networks using Ethernet switches. Control network A connects to the primary IPSIs, and control network B connects to the secondary IPSIs (Figure 22: S8700-series fiber-PNC control network).

Figure 22: S8700-series fiber-PNC control network



Circuit packs that support IP signaling and media traffic

Figure 23: S8700-series / MCC1 signaling path

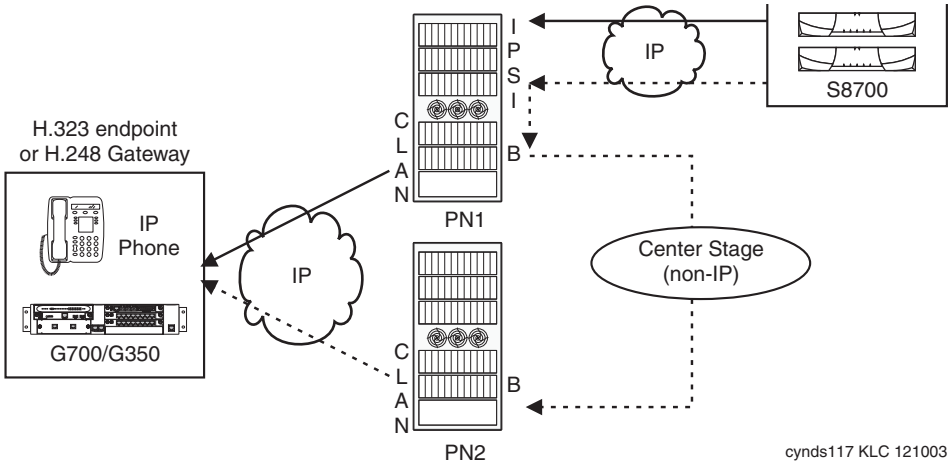
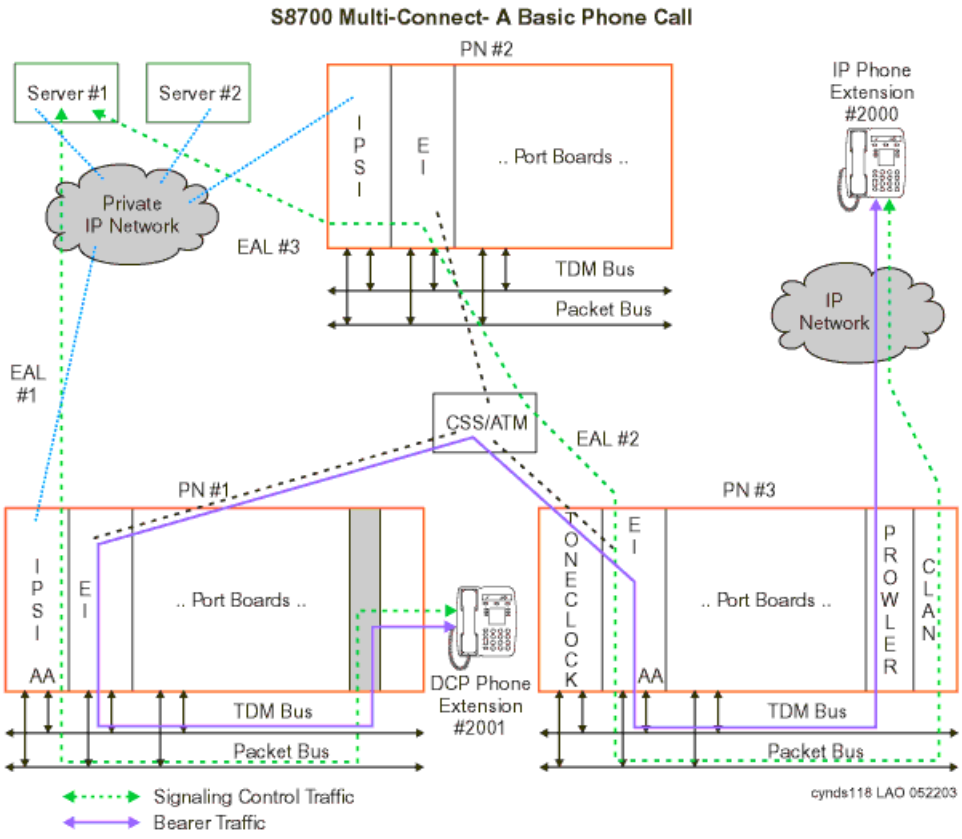


Figure 24: S8700-series fiber-PNC — a basic phone call



IP Server Interface (TN2312BP) - The IP Server Interface (IPSI) is the communication interface between the server and the Media Gateways (port networks). The IPSI is responsible for gateway control, and for tunneling call control messages back to the S8700.

One IPSI circuit pack is required per IPSI-connected Media Gateway for standard reliability. Duplicated IPSI circuit packs are required per IPSI-connected Media Gateway for high reliability and critical reliability.

The IPSI is located in the tone/clock slots, and provides the following functions:

- PKTINT packet bus interface
- Archangel TDM bus interface
- Tone/Clock functionality found on the TN2182B Tone/Clock circuit pack
- Ethernet interface for technician access
- Ethernet interface for connectivity to Services laptop computers
- Maintenance board interface for communication with the EPN maintenance board

Each IPSI typically controls up to five gateways by tunneling control messages over the center stage (TDM) network to the PNs that do not have IPSIs. For locations with high IP Telephone traffic, Avaya recommends a greater number of IPSI circuit packs.

An IPSI cannot be placed in:

- A PN that has a Stratum-3 clock interface
- A remote PN that uses a DS1 converter
- A Survivable Remote Expansion Port Network (SREPN)

The IPSI supports the following functions:

- Supports eight global Call Classification ports
- Supports network diagnostic capabilities
- Provides PN clock generation and synchronization for Stratum-4 type II only
- Provides PN tone generation
- Provides distributed PN packet interface
- Supports the download of IPSI firmware
- Provides serial number support for License File feature activation

Control LAN (TN799DP) - The TN799DP Control LAN (C-LAN) circuit pack acts as front-end processor and concentrator and provides the gateway between the public IP Telephony network and the S8700-system. All H.323 signaling messages between IP Telephony endpoints and the S8700-series Servers must pass through the C-LAN. The connectivity path between the IP endpoint and the server is as follows:

Endpoint ⇔ IP Network ⇔ C-LAN ⇔ PN backplane ⇔ IPSI ⇔ IP network ⇔ S8700

The C-LAN circuit pack is used for all IP call signaling for both IP trunks and stations. This circuit pack also provides TCP/IP connectivity to such adjuncts and synchronous applications as Call Management System (CMS) and INTUITY AUDIX.

This circuit pack also supports firmware download capability for all firmware-downloadable circuit packs in a PN, which allows administrators to remotely update the firmware or application code of circuit packs such as the TN799DP (C-LAN) or TN2302AP Media Processor.

The S8700-series platforms support a maximum of 64 C-LAN circuit packs per system (106 on the extra large or XL configuration of the S8720 Server). The number of C-LAN circuit packs that are required depends on the number of IP endpoints that are connected, and the options that the endpoints use. For example, it might be advantageous to segregate IP voice control traffic from device control traffic.

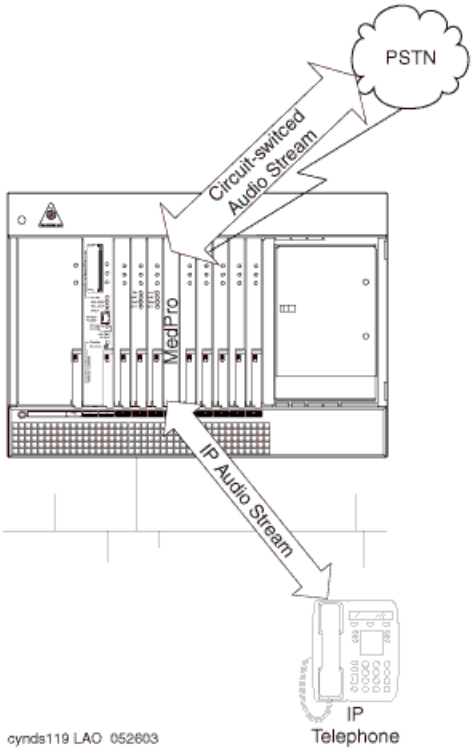
IP Media Processor (TN2302AP, TN2602AP) - The TN2302AP IP Media Processor and the TN2602AP IP Media Resource 320 circuit packs are media processors that provide gateways between the TDM bus and the Ethernet network for audio streams.

Configurations using the S8700-series Servers require resources on TN2302AP and/or TN2602AP media processor circuit packs for IP Telephony bearer communications. TN2302AP and TN2602AP each include a 10/100 BaseT Ethernet interface to support IP trunks and H.323 endpoints. Media processor circuit packs can perform echo cancellation, silence suppression, dual-tone multi-frequency (DTMF) detection, and conferencing.

As shown in Figure 25: TN2302AP Media Processor operation on page 87, the media processor converts circuit-switched audio streams to packet-switched streams. The media processor supports multiple codecs, so it can compress audio samples during packetization. When needed for conference calls, it can also take multiple audio streams, sum them together, and send the resulting audio stream to multiple recipients on the network. Note that the TN2602AP uses the same media processor principles as the TN2302AP.

Starting with release 3.1 of Communication Manager, the TN2602AP IP Media Resource 320 can be duplicated to provide critical bearer reliability for IP-connected port networks.

Figure 25: TN2302AP Media Processor operation



To do the job, a media processing circuit pack has a set of DSP resources. These resources are deployed dynamically and flexibly to any of a number of tasks, including:

- Originating and terminating IP-based packet-switched audio streams
- Establishing and maintaining an RTCP control channel for each IP audio channel
- Compressing and decompressing audio (for example, G.729 to G.711)
- Terminating TCP for an incoming T.120 data stream, and transcoding it to H.221-compliant format for transmission onto the TDM bus and vice-versa
- Summing multiple audio channels into a composite signal for audio conferencing

The S8700 (or S8710) Server is responsible for sending messages to the circuit pack to allocate and to configure the DSP resources to the required task and connecting multiple resources into a chain that performs the desired media processing function. In addition, the server sends the information to the destination of these audio streams.

Since H.323 allows any of several different codecs to be used for encoding an audio stream on the IP network, the Media Processor board is able to use any of the following codecs:

- G.711
- G.723.1
- G.726 (on the TN2602AP circuit pack only)
- G.729 (A, B)

In the same way that a Media Processor board interfaces with IP Telephony endpoints, it can connect to another Media Processor board to interconnect two or more Avaya switches in an IP network over an IP trunk.

Media Gateways

The MCC1, SCC1, and G650 Media Gateways are supported in a fiber-PNC configuration.

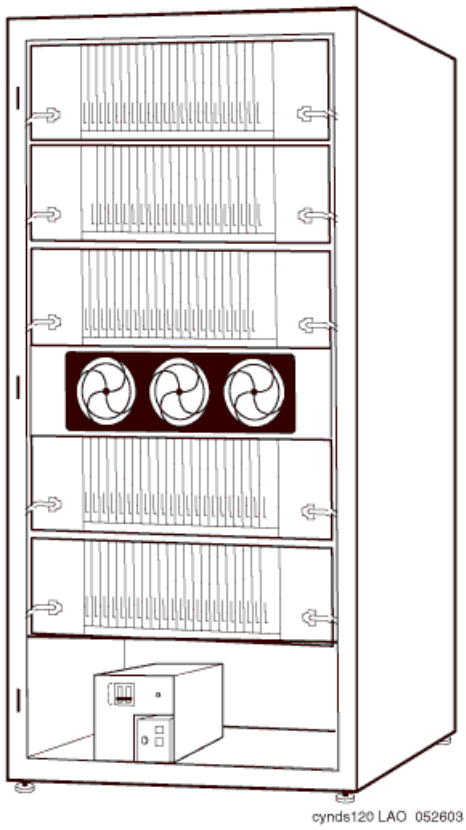
An S8700-series fiber-PNC configuration can have a mixture of MCC1 and SCC1 cabinets. However, the type of cabinet cannot be split within a Port Network.

Multi-Carrier Cabinet (MCC1) Media Gateway - The MCC1 Media Gateway can contain up to five of the following carriers:

- A Port Carrier that contains one or more of the following:
  - Port circuit packs
  - VOIP conversion resources
  - Service circuit packs
  - Tone clocks
  - Expansion Interface (EI) circuit packs
- A Switch Node Carrier that contains Switch Node Interface circuit packs that compose the Center Stage Switch (CSS).
- An Expansion Control Carrier that contains service slots and port slots.

The MCC1 Media Gateways can support a maximum of 98 trunk or line port circuit packs.

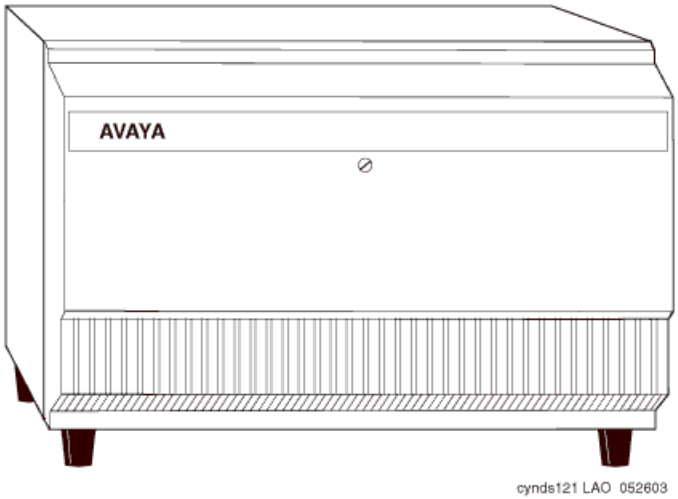
Figure 26: MCC1 Media Gateway



Single-Carrier Cabinet (SCC1) Media Gateway - The SCC1 Media Gateway consists of a single carrier. Up to four SCC1 Media Gateways can be connected together in one location to form one port network. There are two types of SCC1 Media Gateways:

- An Expansion Control Cabinet that contains service slots and port slots.
- A Port Cabinet that contains ports and interfaces to an Expansion Control Cabinet.

Figure 27: SCC1 Media Gateway



Non-IPSI connected Media Gateway - Typically, one of every five Port Networks (PNs) contains one or two IPSI circuit packs. The remaining PNs are referred to as *non-IPSI connected*. Non-IPSI connected PNs get their control information from the servers through one of the PNs that does contain an IPSI. Such control messages are “tunneled” through the circuit-switched network. The system software controls this communication and allocation. The software automatically routes the control messages through an appropriate IPSI. There is no need to administer which IPSI controls the non-IPSI connected PNs. The system automatically allocates those resources, and also compensates for any component failure.

Remote MCC1/SCC1 Media Gateways - The control network for an S8700 with MCC1 or SCC1 Media Gateway can be extended to an IPSI in a remote media gateway. But for cost effectiveness and straightforward installation, Avaya recommends that all of the IPSI-connected media gateways be collocated with the S8700 and Ethernet switches. The circuit-switched network dictates the available options.

Non-IPSI connected media gateways’ circuit-switched network can be extended through all the options available with DEFINITY G3r. Center Stage Switch configurations can use fiber extenders or DS1-Converter (DS1-C) facilities, allowing the media gateway separation to be essentially limitless. When ATM-PNC is used, the media gateway separation is also essentially limitless (see ATM network on page 91).

Remote G700, G450, G350, G250, or G150 Media Gateway - The S8700-series Server can provide the call processing features for a remote G700, G450, G350, or G250 media gateway over an H.248 link, and G150 gateway using H.323. In this configuration, the S8700 can support up to 250 G700, G450, 350, 250, or 150 Media Gateways. An S8300 media module that is located in a G700, G450, G350, or G250 Media Gateway in a remote location provides survivability when the primary controller is inaccessible. For more information, see S8300 as an LSP on page 43.

Another option for survivability of remote gateways is an S8500 Server configured as a Local Survivable Processor (LSP).

Center Stage Switch

The Center Stage Switch (CSS) is a connection hub that provides inter-port network communication between four or more port networks. Often, the CSS is incorporated into smaller configurations to allow for growth. The CSS consists of from one to three switch nodes (SN), which reside in a Port Network carrier. SNs are composed of one or two switch node carriers, depending on whether the solution is being duplicated for critical reliability. Port Network expansion depends on internal SN-to-SN traffic, according to the following guidelines:

- 1 SN expands from 1 to up to 15 PNs.
- 2 SNs expands to up to 29 PNs.
- 3 SNs expands to up to 44 PNs.

ATM network

The Asynchronous Transfer Mode (ATM) switch is a replacement option for the CSS, or for the direct-connect switch. Several Avaya ATM switch types can provide Port Network connectivity. Non-Avaya ATM switches that comply with the ATM standards that are set by the European Union can also provide Port Network connectivity.

ATM-Port Network Connectivity (ATM-PNC) allows any ATM switch or ATM network that complies with specified standards and capacities to serve as the means to connect to the PNs. In this type of configuration, the ATM switch or network replaces the CSS. ATM-PNC is used to connect port networks within a single switch. The WAN Spare Processor (WSP) is not supported. One ATM supports up to 64 PNs.

S8700-series fiber-PNC configuration for higher availability

When used with the MCC1 and SCC1 Media Gateways, the S8700-series Server has the following reliability options:

- Standard reliability configuration
- High reliability configuration
- Critical reliability configuration

Standard reliability configuration

The standard reliability option is the most basic option, which consists of the following components:

- Two S8700-series Servers
- Server-to-IPSI control is not duplicated
- One UPS unit for each S8700-series Server. Using two UPS units ensures that a single UPS failure or repair operation does not disable the system.
- One IPSI in each IPSI-connected port network
- Circuit-switched traffic between port networks is carried on a simplex network that is made up of one Expansion Interface (EI) in each port network. The EIs are cabled with lightguide fiber to either the Center Stage Switch (CSS) or an Asynchronous Transfer Mode (ATM) switch.

Figure 28: S8700-series fiber-PNC in a standard reliability configuration on page 93 shows an example of a standard reliability configuration.

Figure 28: S8700-series fiber-PNC in a standard reliability configuration

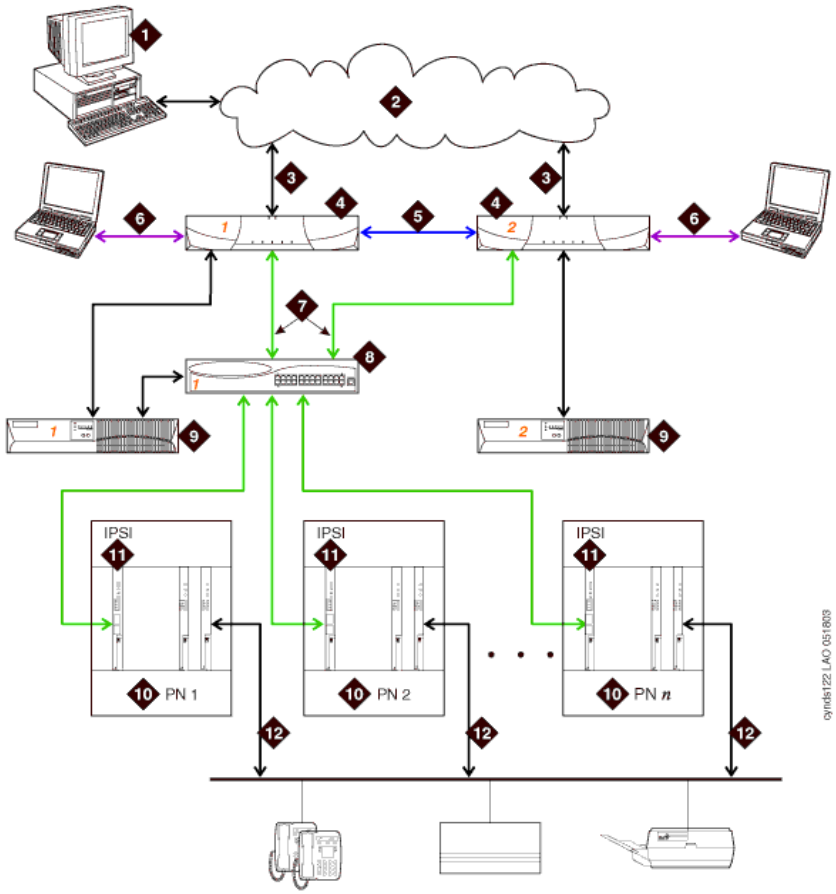


Figure notes:

1. **The Administration PC accesses the S8700-series Server over the corporate data network.**
2. **Corporate IP network.**
3. **Corporate IP network interface. The Ethernet 4 link from the S8700 to the data network.[1]**
4. **Two S8700s are always present. One server is in active mode, and the other server is on standby.**
5. **Duplication interface, default Ethernet 2. The dedicated Ethernet connection between the S8700-series Servers.**
6. **Services interface, default Ethernet 1. The server's dedicated Ethernet connection from the S8700 to a laptop computer (active only during on-site administration or on-site maintenance).**
7. **Network control A interface, default Ethernet 0. The server's Ethernet connection to one or two Ethernet switches. This Ethernet link carries the control signals for the PNs.**
8. **Ethernet switch. At least one Ethernet switch is required to support the control network. If many PNs are present, two Ethernet switches can be daisy-chained together to provide sufficient Ethernet connections to the IPSI boards in the PNs.**
9. **UPS. Keeps the S8700-series Servers and the Ethernet switches functional during brief power outages.**
10. **Port networks.**
11. **IPSI. The IPSI circuit pack carries the control network signals to the PNs, and provides tone clock functionality.**
12. **Bearer connectivity over Center Stage Switch or ATM.**

1. The Ethernet connection to the corporate network in this figure is a nondedicated network. IP addresses for the various components of the S8700-series fiber-PNC configuration must be administered to prevent conflicts with other equipment that shares the network. In the default S8700 fiber-PNC configuration, all other Ethernet connections operate on their own closed LANs.

High reliability configuration

The high reliability configuration option builds on the standard reliability option. The high reliability option duplicates components, so that no single point of failure exists in the control network. The high reliability configuration consists of the following components:

- Two S8700-series Servers
- Two IPSI circuit packs in each IPSI-connected port network
- Two Ethernet switches
- Two UPS units

Circuit-switched traffic between port networks is carried on a simplex network that is made up of one Expansion Interface (EI) in each port network. The EIs are cabled with lightguide fiber to either the Center Stage Switch (CSS) or an Asynchronous Transfer Mode (ATM) switch.

Figure 29: S8700-series fiber-PNC in a high reliability configuration on page 95 shows an example of a high reliability configuration.

Figure 29: S8700-series fiber-PNC in a high reliability configuration

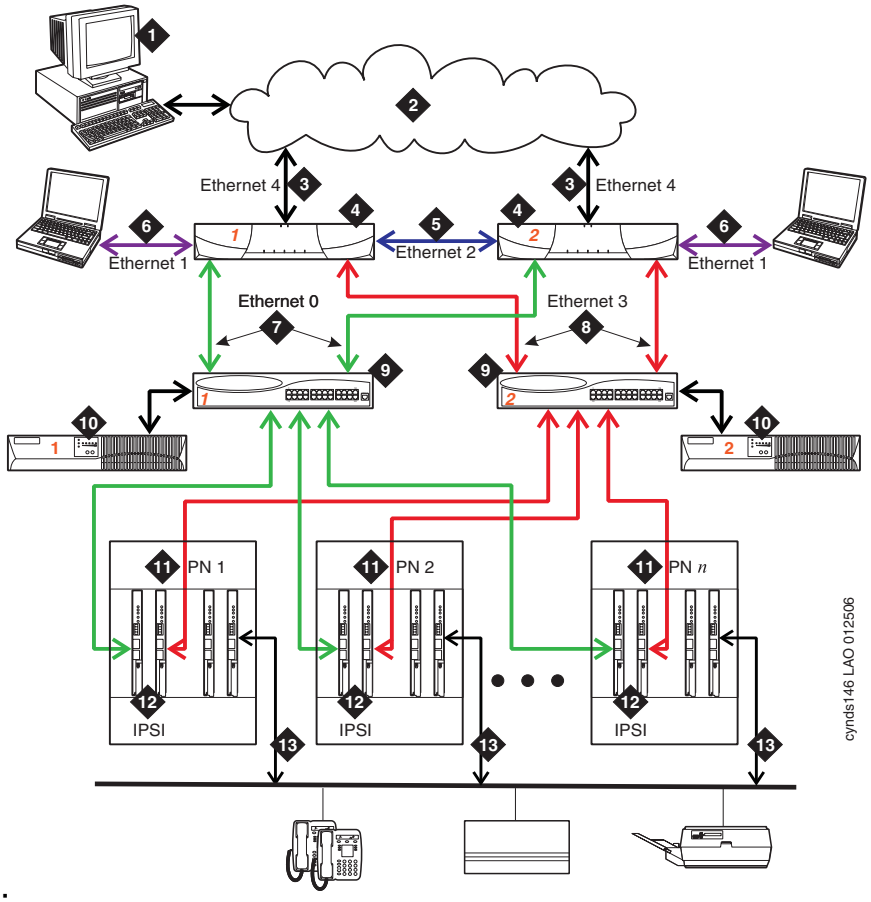


Figure notes:

1. **The Administration PC is used to access the S8700-series Server over the corporate data network.**
2. **Corporate IP network.**
3. **Corporate IP network interface. The Ethernet 4 link from the S8700-series Server to the data network.[1]**
4. **Two S8700-series Servers are always present. One server is in active mode, and the other server is on standby.**
5. **Duplication interface, default Ethernet 2. The dedicated Ethernet connection between the S8700-series Servers.**
6. **Services interface, default Ethernet 1. The server's dedicated Ethernet connection from the S8700-series Server to a laptop computer (active only during on-site administration or on-site maintenance).**
7. **Network control A interface, default Ethernet 0. The server's Ethernet connection to one or two Ethernet switches. This Ethernet link carries the control signals for the PNs.**
8. **Network control B interface, default Ethernet 3. The server's Ethernet connection to one or two Ethernet switches. This Ethernet link carries the control signals for the PNs.**
9. **Ethernet switches. If many PNs are present, two Ethernet switches can be daisy-chained together to provide sufficient Ethernet connections to the IPSI boards in the PNs.**
10. **Duplicated UPSs. Keeps the S8700-series Servers and the Ethernet switches functional during brief power outages.**
11. **Port Networks.**
12. **Duplicated IPSI circuit packs**

1. The Ethernet connection to the corporate network in this figure is a nondedicated network. IP addresses for the various components of the S8700-series fiber-PNC configuration must be administered to prevent conflicts with other equipment that shares the network. In the default S8700 fiber-PNC configuration, all other Ethernet connections operate on their own closed LANs.

Critical reliability configuration

The critical reliability configuration option is built upon the high reliability configuration. In the critical reliability configuration, the bearer network has duplicated components so that there is no single point of failure. The critical reliability configuration consists of the following components:

- Two S8700-series Servers
- Two IPSI circuit packs in each IPSI-connected port network
- Two Ethernet switches
- Two UPS units
- Two CSS/ATM EI (Expansion Interface) in every port network

S8700-series fiber-PNC survivability

In addition to the high reliability of the duplicated S8700-series Servers, the S8300 or S8500 Server in a Local Survivable Processor (LSP) configuration can be used to provide survivability for H.248 branch gateways and IP phones. Additional recovery capability is embedded in the Communication Manager that resides on the S8700-series Server.

The S8500 and S8700-series Servers provide survivability for remote G650 Media Gateways and port networks with IPSI.

Avaya S8700-series Server IP-PNC configuration

The S8700 IP-PNC configuration is an all-IP solution that is built on open IP network connection. This solution is designed for medium to large enterprises. The main difference between the IP-PNC and fiber-PNC configurations is that IP-PNC uses the IP network for all inter-port network communication whereas fiber-PNC uses optic-fiber connections between the PNs in a CSS or ATM network.

The IP-PNC platform is scalable to 64 Port Networks, each of which can house up to five G650s and up to 250 G700, G450, G350, G250, or G150 Media Gateways. The server complex still consists of duplicated S8700-series Servers. One server is active, and the other server is on standby. See Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities on page 34 for information on the S8700-series Server performance and capacities.

Figure 30: Avaya S8700-series Server with remote G650 / G700 / G350 Media Gateways on page 97 shows an example of an S8700 with remote G700 Media Gateways.

Figure 30: Avaya S8700-series Server with remote G650 / G700 / G350 Media Gateways

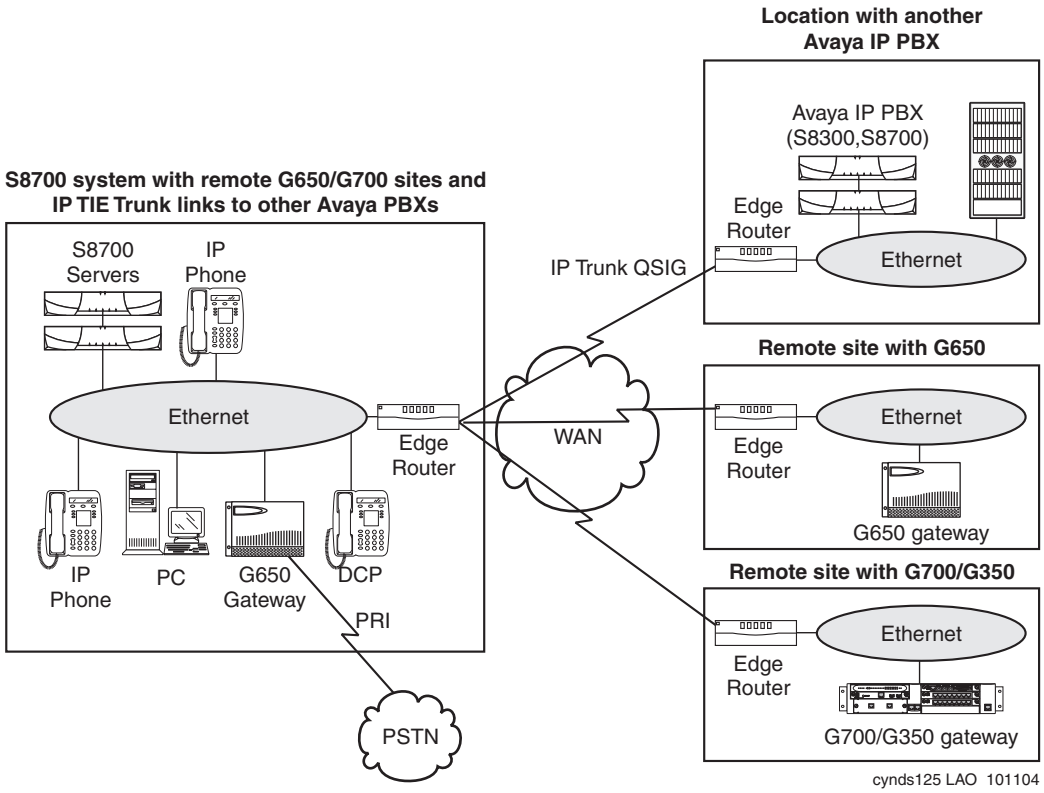
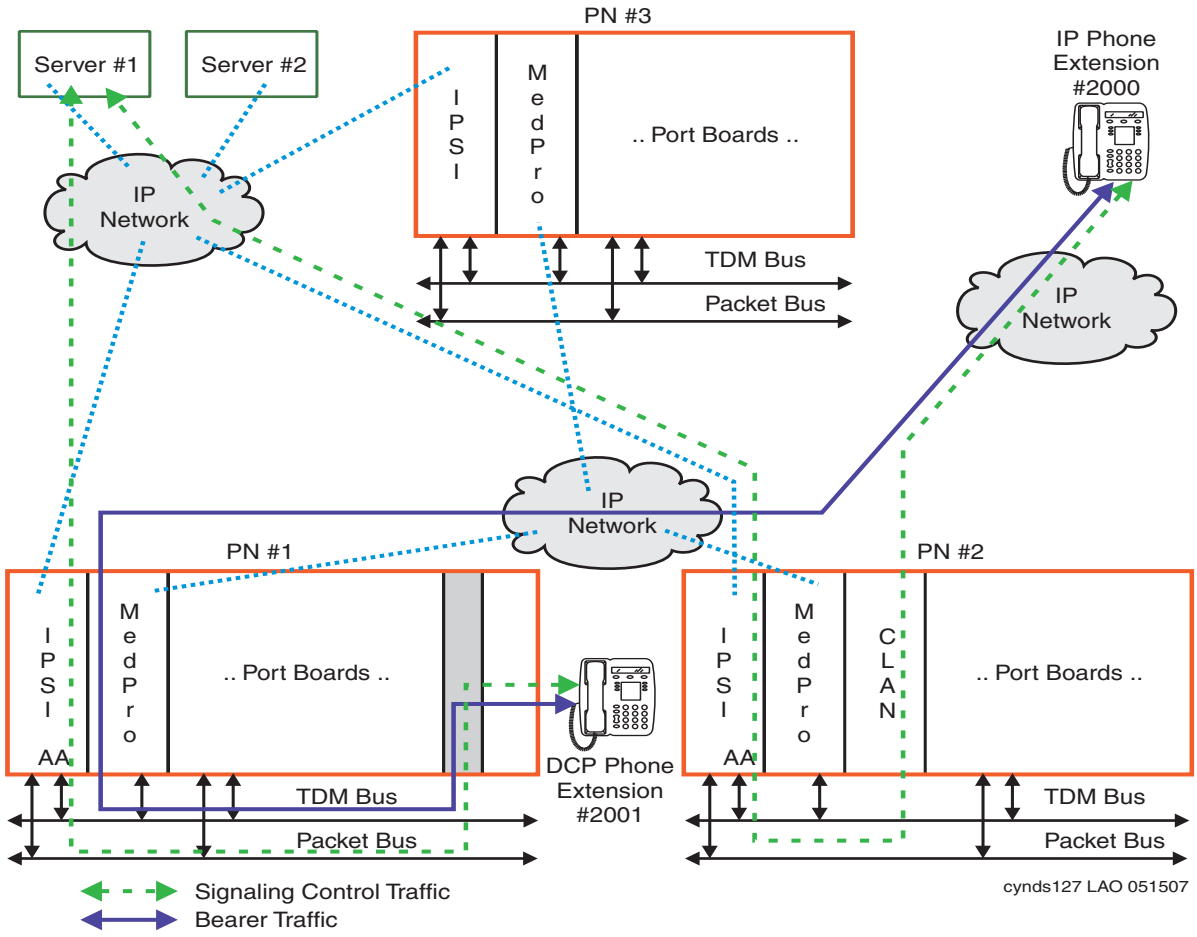


Figure 31: S8700-series Server IP-PNC — a basic phone call on page 98 shows a call through an S8700 IP-PNC system.

Figure 31: S8700-series Server IP-PNC — a basic phone call



Main components

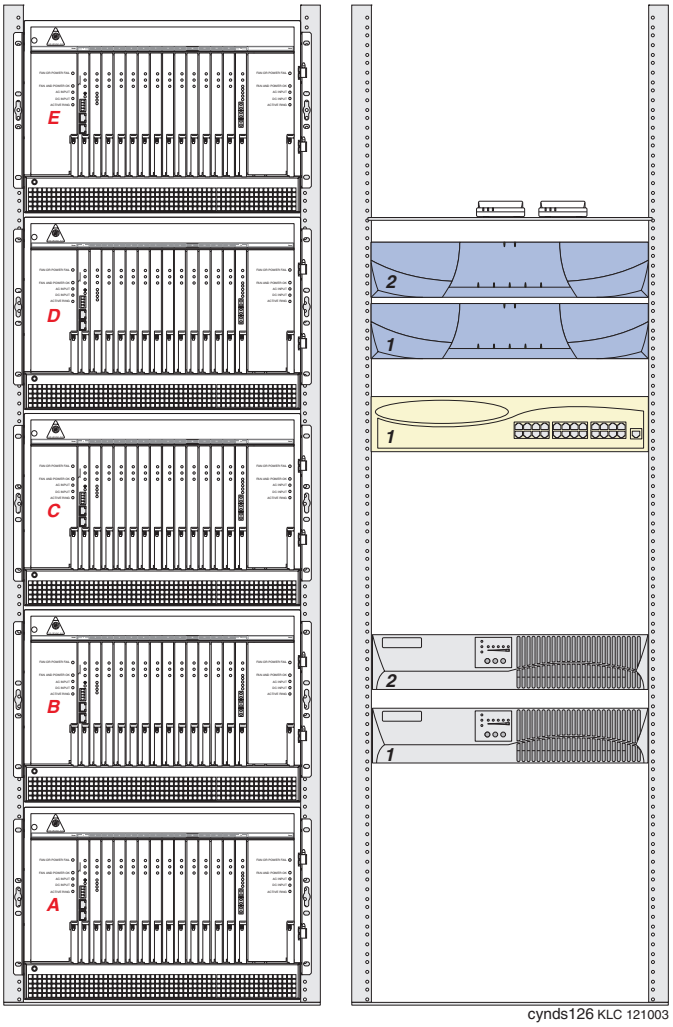
The S8700-series Server IP-PNC consists of the following main components:

- Duplicated S8700-series Servers
- Two UPS units, one for each server
- Two Abstract Control Modem (ACM) compliant Universal Serial Bus (USB) modem
- At least one IPSI per port network
- TN799DP C-LAN (for IP endpoint signaling)

- At least one TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 to support inter-PN and intra-PN connectivity
- The G650 Media Gateway
- Avaya Communication Manager

Figure 32: S8700-series Server IP-PNC major components on page 99 shows the main S8700 IP-PNC components mounted in an open EIA-310-D- compliant, 19-inch data rack.

Figure 32: S8700-series Server IP-PNC major components



The left data rack contains a stack of five G650 Media Gateways that are labeled A through E.

The right data rack contains the following (from top to bottom):

- Two USB-compliant modems
- Two S8700-series Servers
- One Avaya Ethernet switch
- Two AS1 UPS units

S8700-series IP-PNC reliability configurations

The S8700-series Servers are duplicated. The control and IP-bearer links can also be duplicated. The clock functionality is provided by the IPSI circuit pack in each port network. As an all-IP solution, the S8700 IP-PNC only supports IP media gateways. The S8700 IP-PNC does not support traditional CSS- or ATM-connected media gateways.

Starting with release 3.1 of Communication Manager, the capabilities of the TN2602AP IP Media Resource 320 have been expanded to provide duplicated bearer support. This enables customers to administer IP-PNC with critical bearer reliability. A port network continues to support a maximum of two TN2602AP circuit packs but they can now be administered for duplication, in addition to the previously offered load balanced support.

S8700 IP-PNC configuration

Figure 33: S8700 IP-PNC standard configuration

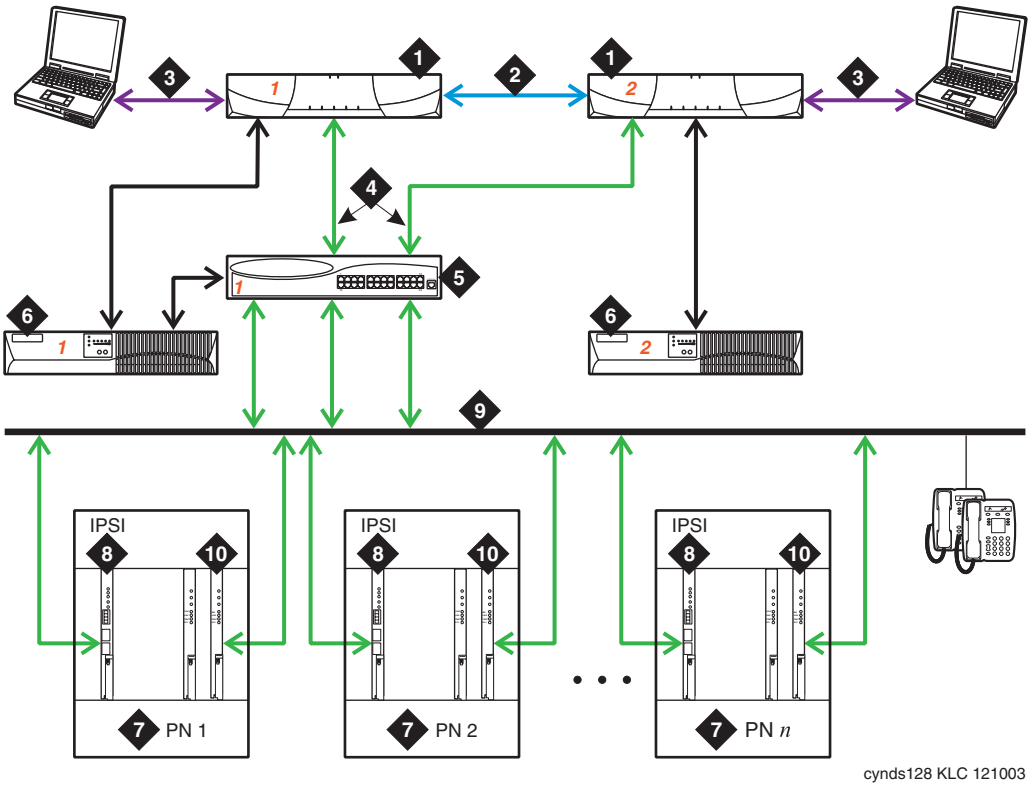


Figure notes:

1. Two S8700-series Servers. One server is in a active mode, and the other server is on standby.
2. Duplication Interface. The Ethernet connection between the two S8700-series Servers.
3. A dedicated Ethernet connection to a laptop computer. This connection is active only during on-site administration or maintenance, and the Services interface can link to the non-active server through a telnet session.
4. Connection from the servers to the Ethernet switch.
5. Ethernet switch. A device that provides port multiplication on a LAN by creating more than one network segment.
6. UPS units. Two UPS units are required
7. Port Network. An optional configuration of Media Gateways that provides increased port capacity.
8. IPSI. A circuit pack that transports control messages over IP. The IPSI circuit pack is used so that the S8700-series Server can communicate with the Port Networks.
9. Customer LAN.
10. TN799DP Control-LAN (C-LAN)

Combined IP and fiber Port Network Connectivity

Communication Manager Release 3.0 enables the S8700-series and S8500 Servers to support configurations that combine IP-connected port networks (IP-PNC) with fiber-connected port networks (fiber-PNC).

Note:

Fiber-PNC configurations include direct-connected, CSS-connected, and ATM-connected port networks (PNs).

Additionally, in combined IP-PNC and fiber-PNC configurations with the S8700-series Server, customers have the option of either single or duplicated control networks.

Combined IP-PNC and fiber-PNC configurations allow the following:

- Add IP-connected PNs to a fiber-PNC configuration using the simpler, less costly connections over the customer LAN.
- Convert and consolidate, in an easy cost-effective way, remote standalone DEFINITY servers (SI, CSI, or S8100) and their PNs into a single network of PNs controlled by, and administered with, one server.
- Configure, within the single footprint of an MCC1 Media Gateway, multiple port networks using IP-PNC, fiber-PNC, or a variety of combinations of the two. In this way, customers have tremendous flexibility in configuring MCC1 Media Gateways to balance reliability, call capacities, and feature richness.
- Configure reliability into a network in a more cost-effective, flexible way. Duplication of control can be configured based on the criticality of the location or the needs of users connected to a particular PN.

Combined IP-PNC and fiber-PNC configurations support the following platforms:

- S8500 and S8500B servers in both IP-PNC and direct-connect configurations with CMC1, MCC1, SCC1 and G650 Media Gateways
- S8700-series Server pairs in IP-PNC and direct-connect configurations with CMC1, MCC1, SCC1 and G650 Media Gateways
- S8700-series Server pairs in both IP-PNC and fiber-PNC with either CSS or ATM configurations and CMC1, MCC1, SCC1 and G650 Media Gateways

Note:

A single combined IP-PNC and fiber-PNC system cannot have a mixture of connection types in the fiber-PNC segment. The port networks in the fiber-PNC segment must be all direct-connected or all CSS-connected or all ATM-connected.

The G650, SCC1, and MCC1 Media Gateways can connect to a combined IP-PNC and fiber-PNC system using either IP or fiber connections. The CMC1 Media Gateway can be IP-connected only and cannot be fiber-connected in any of the combined IP-PNC and fiber-PNC configurations. The following table lists, by server, the media gateways and connection methods that can be simultaneously supported in a combined IP-PNC and fiber-PNC configuration.

Server	Supported Central Gateways	IP-Connect	Direct-Connect	CSS/ATM-Connect[1]	Reliabilities Supported
S8500/ S8500B	CMC1	yes	no	no	single control and bearer only
	G650	yes	yes	no	same as CMC1
	SCC1	yes	yes	no	same as CMC1
	MCC1	yes	yes	no	same as CMC1
S8700 series	CMC1	yes	no	no	single control, single bearer only
	G650	yes	yes	yes (requires an MCC1 for CSS)	• single control and bearer • duplicated control only • duplicated control and bearer
	SCC1	yes	yes	yes (requires an MCC1 for CSS)	same as G650
	MCC1	yes	yes	yes	same as G650

1. For any system, either CSS or ATM connections may be used in a combined IP-PNC and fiber-PNC network, but not both.

Media Gateway Capacity

The following capacity rules apply to a combined IP-PNC and fiber-PNC configuration:

Each combination of fiber-PNC and IP-PNC can support up to 64 port networks. When the fiber-PNC portion is supported by CSS, it can have a maximum of 44 CSS PNs but the system can be expanded to 64 PNs by adding an additional 20 IP-connected PNs. When the fiber-PNC portion is direct-connect, with two or three direct-connect PNs, the IP-PNC portion can have up to 61 or 62 IP-connected PNs, respectively.

Capacity limit for media gateways

A combined IP-PNC and fiber-PNC system can support up to 250 Media Gateways including the G150, G250, G350, G450, and G700.

Configuration rules

Combined IP-PNC and fiber-PNC requires CM3.0 or later software but does not require any new hardware of firmware changes. The following configuration rules apply to combined IP-PNC and fiber-PNC configurations:

- The current rules for IP-PNC and fiber-PNC (CSS or ATM) continue to apply. For example, if IP-PNC port networks are added to an existing S8700/S8710 fiber-PNC system, every IP-PNC port network must have one active IPSI circuit pack.
- The current rules for IP-PNC and the rules for direct connect continue to apply. In a direct connect system, only one IPSI controls the direct-connect PNs.
- There must be at least one IP Media Processor board (TN2302AP or TN2602AP) in a port network of the fiber-PNC portion of the configuration. The PN or PNs that contain the IP media processor circuit pack act as *gateway port network(s)* between the IP-PNC and fiber-PNC portions of the configuration.

  Note:

  The TN2602AP IP Media Resource 320 Circuit Pack is not supported in CMC1 Media Gateways. The CMC1 supports the TN2302AP IP Media Processor board.
- In an IP-connected port network, tone detectors (call classifiers, etc) must be engineered per port network bases, while in a fiber-connected CSS or ATM cluster, the tone detection resources can be shared over the fiber connected link.
- There must be at least one C-LAN circuit pack in the fiber-connected portion of the configuration.

MCC1 Media Gateway with one or more IP- and fiber-connected PNs

In a combined IP-PNC and fiber-PNC configuration, an MCC1 Media Gateway may contain

- up to 5 fiber-connected PNs.
- up to 5 IP-connected PNs.
- both IP-connected and fiber-connected PNs (this only applies for migration and conversions to CM3.0).
- up to two IP-connected PNs with duplicated control networks.

Thus, both IP- and fiber-connected PNs can exist in a single MCC1 Media Gateway.

The following table is an example of port network configuration options for IP-connected PNs in an MCC1 Media Gateway.

	MCC1 with 3 PNS with single control	**MCC1 with 3 PNS, one with duplicated control**
C Carrier		
B Carrier	IPSI	IPSI
A Carrier	IPSI	IPSI
D Carrier	IPSI	IPSI (Secondary)
E Carrier		IPSI (Primary

Mixed reliability options

The reliability options separately available for each PNC method still apply except that fiber-connected PNs (fiber-PNC) with single control networks cannot be mixed with IP-connected PNs (IP-PNC) with duplicated control networks. To have duplicated control in the IP-PNC portion of the configuration, the fiber-PNC portion must have duplicated control.

The PNs in a mixed fiber-PNC and IP-PNC configuration can collectively have multiple levels of reliability. However, within the fiber-PNC portion of a system (direct, CSS, or ATM-connected PNs), all port networks must have the same reliability level --- all single control and bearer networks, all duplicated control and single bearer networks, or all duplicated control and bearer networks.

The following table summarizes the valid IP-PNC reliability options in a combined IP-PNC and fiber-PNC configuration.

	Connection Method for Mixed PNC Configurations		
	Fiber Port Network Connectivity (Direct-connect/CSS/ATM)		**IP Port Network Connectivity[1]**
Reliability Option	Single control network only	and	Single control network only
	Duplicated control network [2]	and	Single control network only
		and	Duplicated control network[3]
		and	Single control network for some PNs and duplicated control network for other PNs
	Duplicated control network and duplicated bearer network	and	Single control network only
		and	Duplicated control network
		and	Single control network for some PNs and duplicated control network for other PNs. Duplicated IP bearer network.

1. Any of these configurations can also have duplicated IP bearer.

2. Not available with S8500 Servers

3. Only if the fiber-PNC portion has a duplicated control network

Networking option of S8700-series Server pair for duplicated and single control networks

For an S8700-series Server pair with direct/CSS/ATM PNC and duplicated control networks, control network A and control network B interfaces are administered as dedicated control networks and connected to duplicated IPSI circuit packs in the fiber-connected PNs. If a remote IP-PNC PN is introduced into the configuration, the S8700-series Server and IP-PNC PN may be administered for a single non-dedicated control network over the customer's LAN. In this case, a third control network C may be administered on the S8700-series Server. The S8700-series Server automatically uses its own customer LAN interface port for Control network C.

Although this configuration allows the mixing of dedicated and non-dedicated control networks, it is discouraged. It is recommended that same control network to be configured across a combined IP-PNC and fiber-PNC system.

ESS support for combined IP-PNC and fiber-PNC configurations

Any Enterprise Survivable Server (ESS) can also support a combined IP-PNC and fiber-PNC configuration in the event of failover to the ESS. Both an S8500 and an S87XX-series ESS can support single control and duplicated control networks for both the IP-PNC and fiber-PNC portions of the configuration. However, the ESS can support only those CSS-connected PNs that individually have an IPSI circuit pack and either a TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack. This limitation exists because the ESS provides only IP-PNC control and bearer service to PNs.

Processor Ethernet

Processor Ethernet allows IP devices to register to an Avaya server without a need for TN799DP C-LAN boards. Prior to Communication Manager release 3.1, Processor Ethernet was permitted only when using S8300 or Shared Servers (e.g. Hosted IP Telephony). As of release 3.1, Processor Ethernet can also be used with the S8400 and S8500 Servers. Furthermore, as of release 3.1, S8500 can be used as an LSP (Local Survivable Processor).

The following table describes the usage of Processor Ethernet as of release 3.1
:

Table 15: Applications of Processor Ethernet as of Communication Manager release 3.1

Servers	Processor Ethernet Application	Prior to release 3.1	As of release 3.1
Main Servers	H.323 Endpoint Registration	S8300	S8300, S8400, S8500
	H.248 Gateway Registration	S8300	S8300, S8400, S8500
	IP Adjunct Connections	S8300	S8300, S8400, S8500
Simplex ESS Servers	H.323 Endpoint Registration	Not permitted	Not permitted
	H.248 Gateway Registration	Not permitted	Not permitted
	IP Adjunct Connections	Not permitted	Permitted for Selected Adjuncts
LSP Servers	H.323 Endpoint Registration	S8300 LSP	S8300 LSP, S8500 LSP
	H.248 Gateway Registration	S8300 LSP	S8300 LSP, S8500 LSP
	IP Adjunct Connections	Not permitted	Permitted for Selected Adjuncts on S8300 LSP, S8500 LSP

Avaya IP Office

Avaya IP Office is another standalone Avaya platform that supports IP Telephony for the small to mid-size market.

Avaya IP Office is an IP PBX for 10 to180 stations. Avaya IP Office is not part of the Avaya Application Solutions offer, and thus is not covered extensively in this document. For more information about the IP Office, see the Avaya Support website.

Greenfield deployment

This chapter explains how to implement Avaya Application Solutions components in a Greenfield site. A Greenfield site is a business or an organization that does not have an existing communication system. Most Greenfield systems are deployed into new businesses and organizations, and these systems tend to be smaller in size. Occasionally, an established large organization may completely remove its existing system and install a new system. In these cases, the incumbent system is usually a leased service, such as a centrex service from a telephony service provider.

In general, most organizations want to protect their investment in their PBX communications system. Avaya provides ways for our circuit switched PBX customers to evolve from circuit switched systems to IP-enabled systems. This solution provides most of the advantages of IP Telephony with minimal equipment upgrades to an enterprise's existing PBX. The evolution approach is described in Evolution from circuit-switched to IP on page 119.

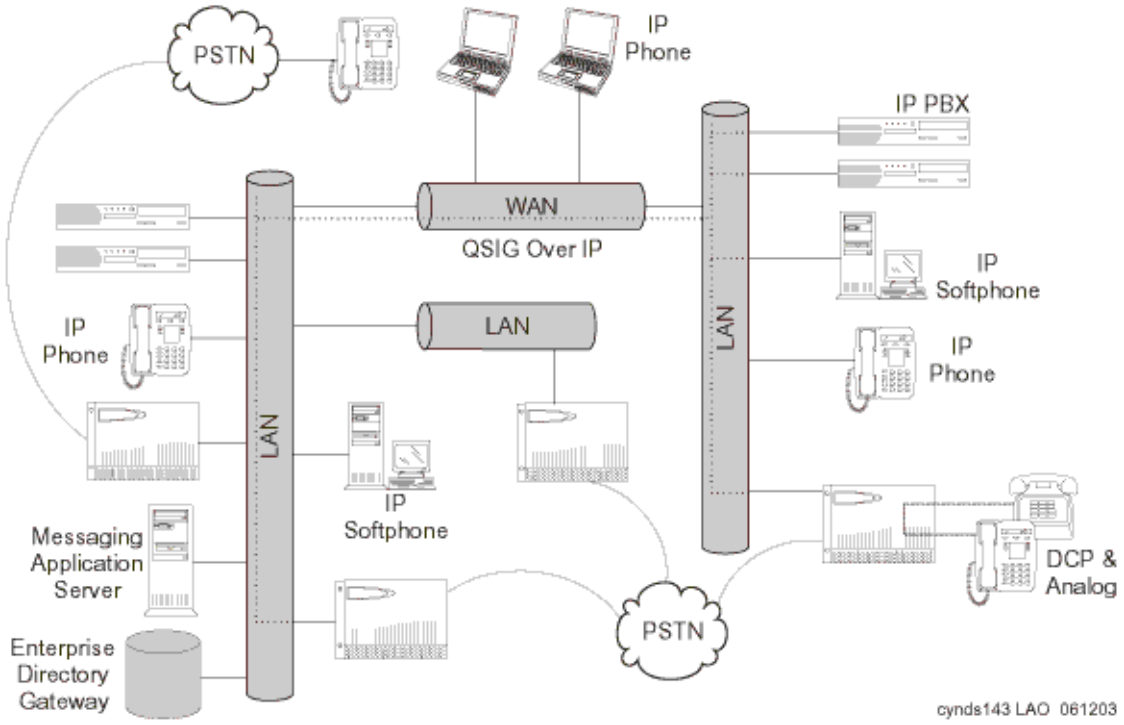
Components needed for Greenfield deployment

In a Greenfield deployment, the primary connection medium is IP. To provide the greatest flexibility and the lowest costs for a converged solution, most endpoints should be IP Telephones or IP Softphones. A mixture of IP endpoints and circuit-switched endpoints places increased demand on Media Processor resources, and thus increases the cost of the deployment. Intersite communications should also be IP based. This can be done either through direct connections between IP Telephones or through IP trunks. Circuit-switched or TDM-based communications should be kept to a minimum. The primary TDM connections should be for PSTN access, where necessary, and connections to any analog telephones, modems, or fax machines that exist (Figure 34: A Greenfield IP Telephony deployment on page 110).

In a Greenfield deployment, the emphasis is on IP Telephony. Multi-Connect systems that emphasize TDM connections are not generally recommended, except in special circumstances. Those circumstances include when there is a need for:

- Critical reliability
- Significant analog or DCP endpoints

Figure 34: A Greenfield IP Telephony deployment



Servers (H.323 Gatekeeper)

The servers are responsible for running Avaya Communication Manager and controlling the Media Gateways and endpoints. The servers control the dial plan translations and call routing, call setup and teardown, Call Detail Record (CDR) generation, traffic management. The servers also offer H.323 gatekeeper functionality, and provide the extensive telephony features that are included with Avaya Communication Manager.

Avaya's Linux-based servers include:

- S8300 Server (The server resides in the G700, G350, or G250 Media Gateway)
- S8400 Server
- S8500 Server
- S8700-series Servers

Avaya Communication Manager

Communication Manager IP capabilities and applications support voice over an IP network, and ensure that remote workers have access to communication system features from their PCs. Communication Manager also provides standards-based control between servers and Media Gateways, which allows the communications infrastructure to be distributed to the edge of the network. The Communication Manager IP engine offers features that enable users to increase the quality of voice communications. Quality of Service (QoS) features enable users to optimize voice quality by assisting some routers in prioritizing audio traffic. Communication Manager Media Processors allow for hairpinning and shuffling. These features make voice communications more efficient by reducing both per-port costs and IP bandwidth usage. Avaya IP Telephony Solutions support trunks, IP communications devices, IP Port Networks, and IP control for Media Gateways.

Avaya IP Telephony Solutions are implemented using various IP Media Processor circuit packs inside the Avaya Media Gateways. The IP Media Processors provide H.323 trunk connections, and H.323 voice processing for IP Telephones. H.323 signaling is handled by a C-LAN circuit pack or native processor Ethernet connectivity. The IP network can be extended across geographically disparate locations. With Communication Manager ISDN, Distributed Communication Services (DCS+), or QSIG services, Communication Manager can extend feature transparency, centralized voice mail, centralized attendant service, call center applications, and enhanced call routing across IP trunks.

For more information on Communication Manager architecture, see the Call processing chapter.

Media Gateways and Port Networks

Avaya Media Gateways support voice and signaling traffic that is routed between circuit-switched networks and packet-switched networks. Avaya Media Gateways support all the applications and the adjuncts that are supported by the Avaya DEFINITY Enterprise Communications Servers, accommodating Call Center and Customer Relationship Management applications, messaging, remote workers, and remote offices. Avaya Media Gateways work with standards-based IP networks, and connect easily with the Public Switched Telephone Network (PSTN). The IP network infrastructure provides support for the communication between the servers and the Media Gateways.

In a Greenfield installation, the recommended gateways are the G150, G250, G350, G650, and the G700. The G650 houses traditional circuit switch boards and boards that support IP Telephony. The G700, G350, and G250 house Avaya Media Modules that provide ports for non-IP endpoints, including analog and DCP telephones. Use the G150 and the G250 gateways for large scale, small-branch deployments (2-8 users each). Avaya recommends using the G250 for high-intensity, critical applications, and using the G150 for more affordable solutions where branches are more loosely coupled to headquarters.

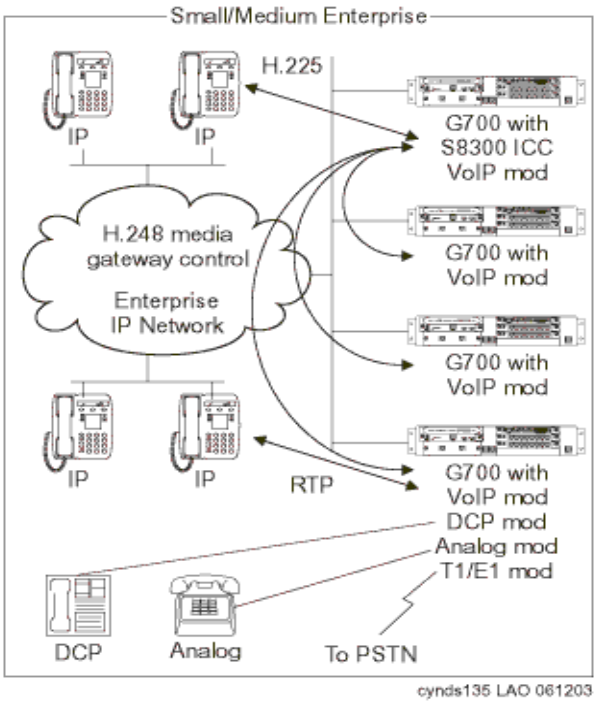
Greenfield configurations

S8300 standalone solution (small-to-midsize enterprise)

An S8300 Server with a G700, G250, or G350 gateway is designed for a small to mid-size office. The S8300 fits into a media module slot in the G700, G350, or G250 Media Gateway. See Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities on page 34 for information on capacities when the S8300 is used with the G700, G350, and G250. An S8300 server does not support G650 gateways or traditional port networks.

As shown in Figure 35: An S8300/G700/G350/G250 system on page 112, the G700 is a 2U 19-inch rack-mountable chassis. The G700 contains a built-in Ethernet switch, an IP expansion module slot, four Media Module slots, and an Octaplane stacking module slot. The built-in IP Telephony module has the same functionality as the TN2302AP Media Processor circuit pack. An extra VoIP Media Module can be inserted in the G700 for extra media-processing resources. Other Media Modules support traditional endpoints.

Figure 35: An S8300/G700/G350/G250 system



Medium-to-large enterprise solutions

Note:

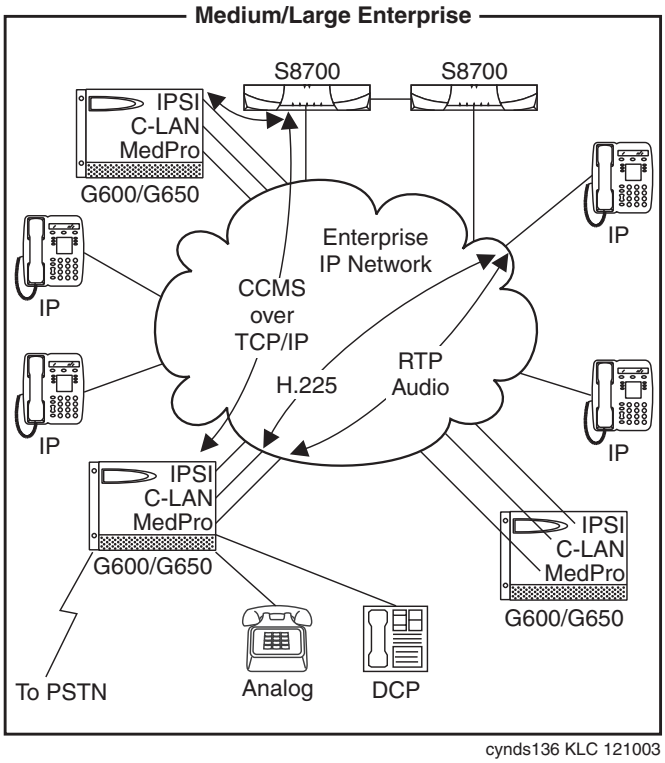
The description of the duplicated S8700-series Server configuration in this section, except for capacities, also applies to an S8500 simplex configuration.

S8700-series / G650 IP-PNC

The S8700-series IP-PNC system (Figure 36: S8700-series IP-PNC system on page 114) is a scalable solution that supports up to 64 G650 Media Gateways in stacks of from one to five rack-mounted G650 cabinets. See Table 4: Avaya Application Solutions comparison matrix — components, performance, and capacities on page 34 for capacities information for the S8700-series IP-PNC system.

The S8700-series Servers can be networked with other systems through IP or circuit-switched trunks to provide for significantly larger telephony networks. The control link between the servers and the Media Gateways traverses the enterprise IP network. All G650 Media Gateways require IPSI circuit packs to provide the Gateway's control link. There is no traditional circuit switch (Center Stage Switch), and the media traffic flow is entirely through the enterprise data network. Each G650 has at least one Media Processor circuit pack, which provides the gateway between the TDM bus and the circuit pack's Ethernet connection for the audio streams. Each G650 also has at least one C-LAN, which provides H.323 signaling to IP endpoints.

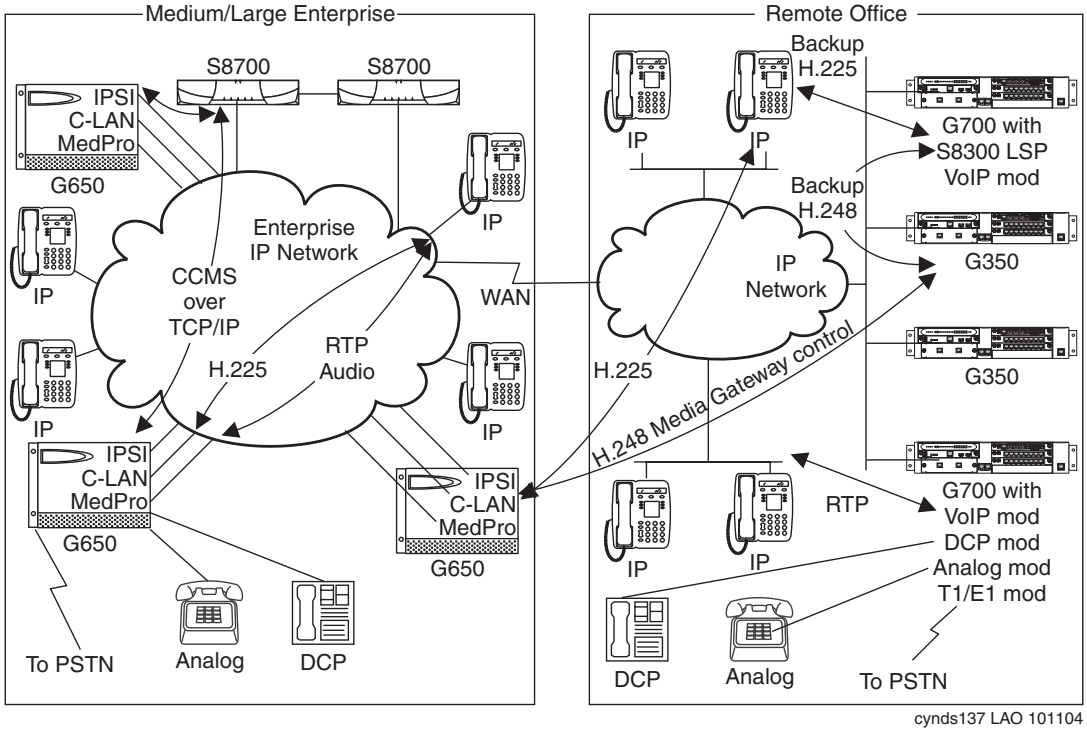
Figure 36: S8700-series IP-PNC system



S8700-series IP-PNC with remote G700s or G350s

The IP-PNC solution can be expanded to support a remote office with G700 or G350 Media Gateways in addition to G650 Gateways (Figure 37: S8700-series IP-PNC with remote G700 or G350s on page 115). This solution is designed for enterprises that require a high number of IP stations, but a low number of PSTN or traditional circuit-switched connections. The S8700-series Server is the call controller that communicates with the G700 or G350 Gateways through the C-LAN. In this configuration, the C-LAN circuit pack acts as the front-end processor for both the G700/G350 Media Gateways and IP endpoints.

Figure 37: S8700-series IP-PNC with remote G700 or G350s



Note:

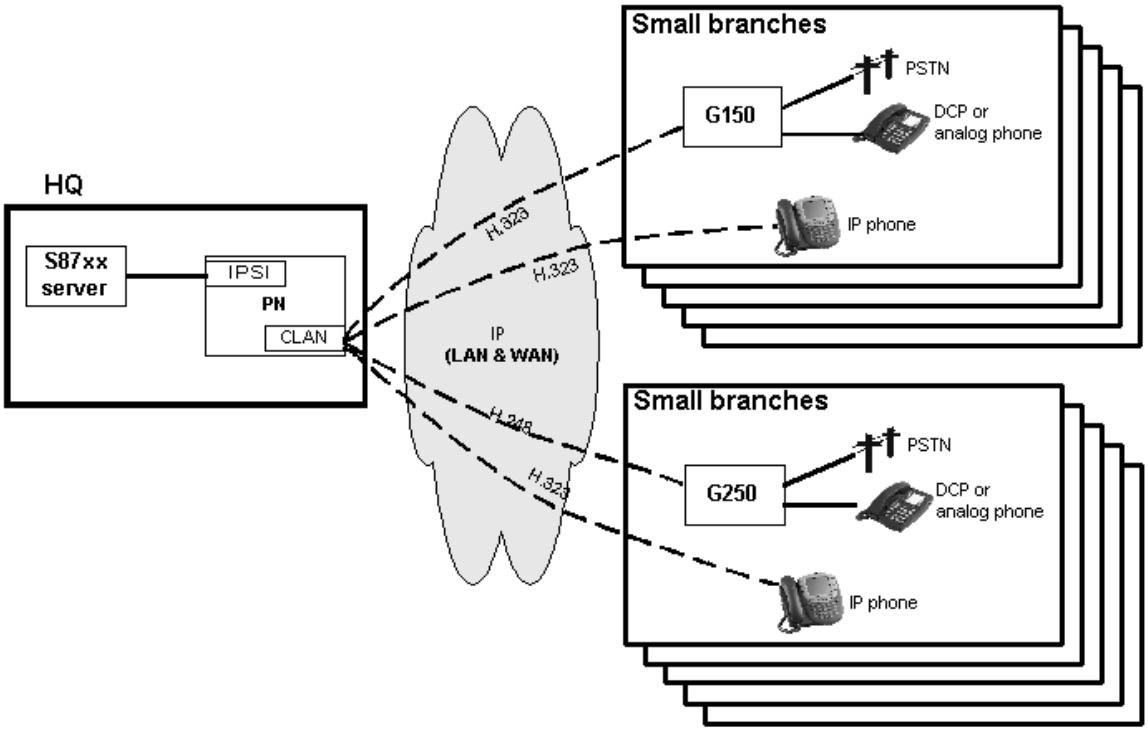
A typical remote office is configured with a single gateway. Several gateways are shown in the remote office in Figure 37 to illustrate additional possible configurations.

S8700-series with G150/G250: large number of remote branches

The newer small gateways G150 and G250 are designed to be deployed individually in large number (100's to 1000's) of small branches, with management and call control centralized at a headquarter with S8700/S8710 servers. Each branch would have a single G150 or G250 with 2-10 stations (analog, DCP, or IP), and analog or T1/E1 PSTN trunks. Any location needing more than 10 stations should consider using G350 or G700. G350 is also meant to be deployed alone at a location; only the G700 should be used in multiple expandable unit configurations.

At each branch, LAN and WAN functions can be provided by external 3rd party or Avaya networking devices, or as part of the integrated options within the gateways. WAN connection back to HQ can utilize low cost options such as VPN over public internet via cable or DSL (G250). Emergency fallback to phone modem is also possible. See Figure 38: S8700-series with G150/G250 -- large number of remote branches on page 116.

Figure 38: S8700-series with G150/G250 -- large number of remote branches



Required circuit packs for S8700-series configuration

The circuit packs that are required for IP Telephony in a Communication Manager system include:

- TN2312BP IP Server Interface (IPSI) for Port Network control. For detailed information, see IP Server Interface (TN2312BP) on page 85.
- TN799DP Control LAN (C-LAN) for signaling and TCP/IP socket termination. For detailed information, see Control LAN (TN799DP) on page 85.
- TN2302AP and/or TN2602AP Media Processors or the media flow. For detailed information, see IP Media Processor (TN2302AP, TN2602AP) on page 86.

These circuit packs can reside in the CMC1, SCC1, MCC1, or G650 Media Gateways in widely-distributed locations.

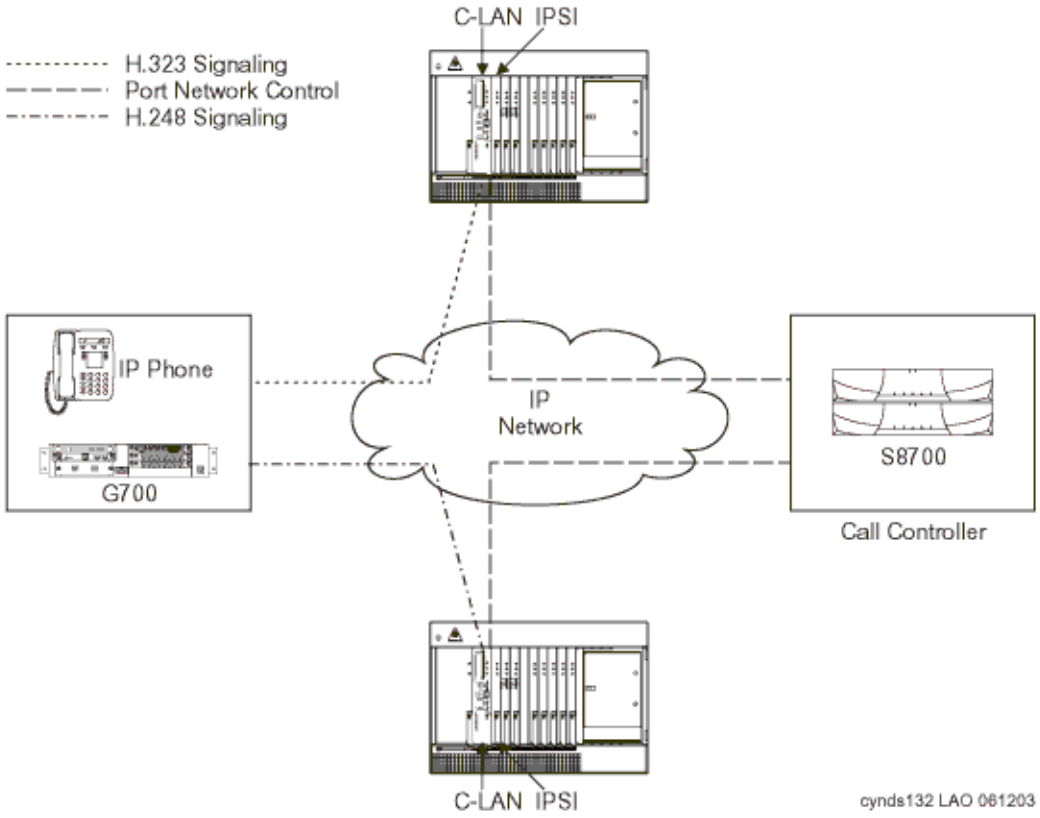
The signaling connectivity path between the endpoint and the servers in the S8700 configuration is shown in Figure 41: Signaling flow on page 118.

As shown in Figure 39: Signaling path (S8700 / G650 configuration) on page 117, an IP Telephone sends all IP Telephony signaling traffic to the C-LAN. The C-LAN multiplexes IP Telephone signaling messages, and sends them to the S8700-series Server through the IPSI.

The connectivity between the endpoint and the server is:

Endpoint ⇔ IP network ⇔ S8300 Server

Figure 39: Signaling path (S8700 / G650 configuration)



Note:

In the IP-PNC S8700 / G650 configuration each Port Network has an IPSI circuit pack.

As Figure 40: Media flow path (S8700 IP-PNC configuration) on page 118 shows, an IP Telephone sends all media streams to the Media Processor board. Once a call is established, if the remote endpoint is another IP Telephone, the media stream might shuffle (be redirected to the other endpoint) without requiring Media Processor resources. Media Processors are also used to transport media streams in IP tie trunks.

Figure 40: Media flow path (S8700 IP-PNC configuration)

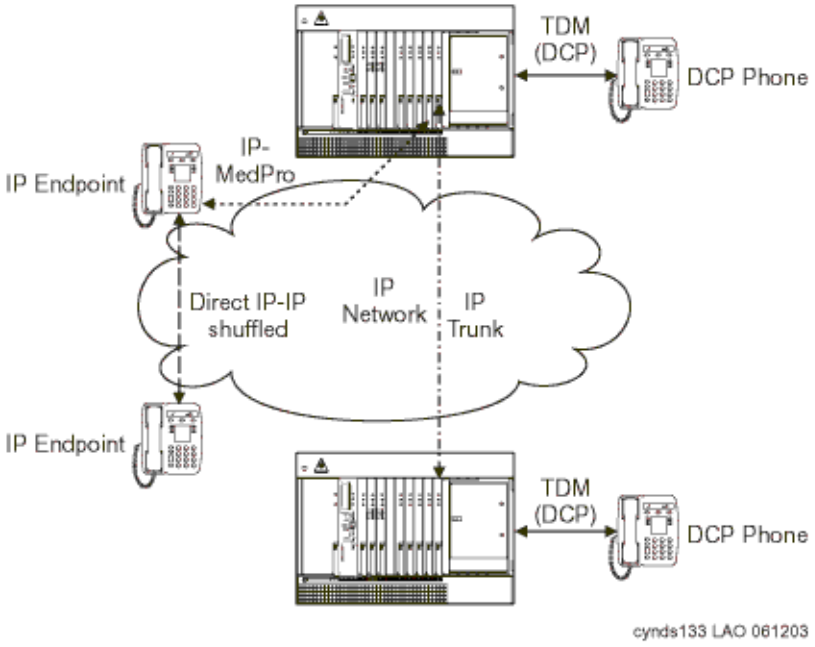
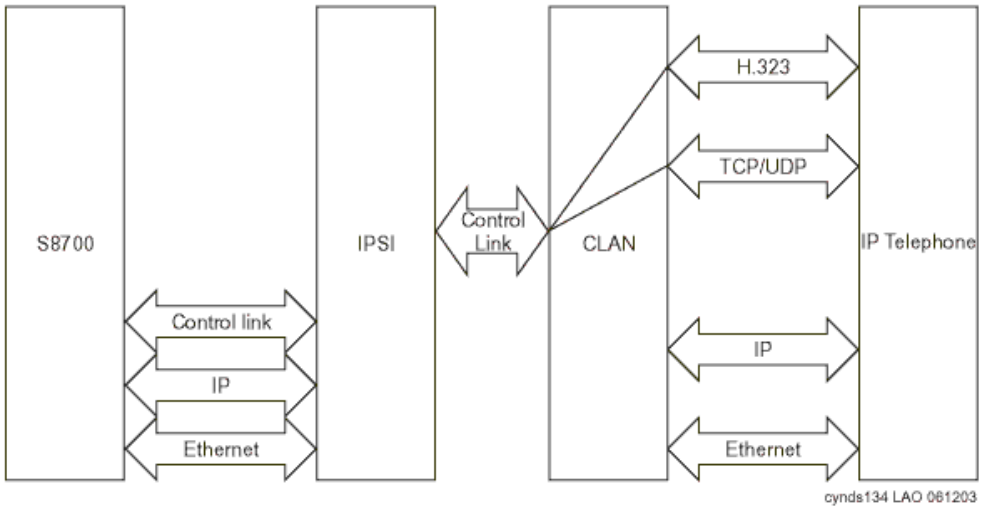


Figure 41: Signaling flow

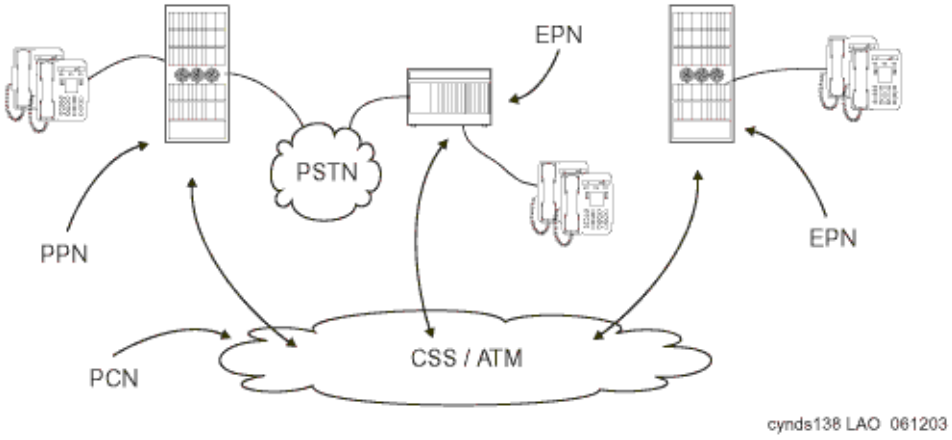


Evolution from circuit-switched to IP

Overview

The Avaya DEFINITY® Enterprise Communications Server G3r has been the flagship product in the DEFINITY family of communications servers. As technology changed, Avaya was able to leverage the rapid advances in microprocessor technology to increase the capacity and processing power of the traditional DEFINITY platform (Figure 42: Traditional DEFINITY configuration) to benefit our customers.

Figure 42: Traditional DEFINITY configuration



Avaya also has the objective to protect our customers' communications investment in the Avaya DEFINITY platform by helping our customers leverage their existing investments in Avaya solutions. Upgrading allows a customer to make a smooth transition to IP Telephony technology without sacrificing the features or reliability of their current DEFINITY. A customer can make small incremental investments to move from the circuit-switched world to a full IP PBX while retaining their investment in TDM-based equipment and connections. On the endpoints, moving to IP Telephony allows simplified moves, adds, and changes. It also simplifies the building wiring plan by sharing one Ethernet connection with both the IP Telephone and the desktop PC. It also adds IP mobility while retaining the rich set of DEFINITY features. For both IP Telephone and traditional circuit-switched telephone users, migrating to IP Telephony offers the opportunity to bypass tolls, and route traditionally metered long-distance calls across an unmetered IP network instead, saving operational costs.

With the S8700 fiber-PNC solution, Avaya is delivering a high-capacity server and a migration path from DEFINITY. The S8700-series Server uses an industry-standard Linux operating system on an industry-standard server, which enables all endpoints to use Communication Manager. This solution allows customers to migrate to IP Telephony and to a higher performance processor without sacrificing the reliability of the G3r platform.

There are three stages to upgrading from a DEFINITY G3r to an Avaya Communication Manager IP PBX:

1. Replace the G3r processor with industry-standard S8700-series Servers.
2. Add IP circuit packs (C-LAN and Media Processor board) to support IP endpoints.
3. Consolidate multiple systems into a single system to simplify administration. Support network or processor failure conditions with LSPs deployed at remote sites.

Steps 1 and 2 can be reversed. The next five diagrams show the migration from circuit-switched DEFINITY to an IP-enabled S8700 fiber-PNC system with server consolidation and LSP survivability at a remote site.

Migration from DEFINITY Server R to S8700 fiber-PNC

Phase 1: Processor replacement

This section explains how an existing non-IP Avaya Communication Manager PBX can evolve to an IP Telephony-based solution. We will examine the case of an existing system that is based on the traditional PPN/EPN architecture, which will be applicable to all the G3 platforms.

When designing S8700 fiber-PNC systems, there are two options for setting up the call control network. The control network can be set up on the enterprise LAN or on a private network that is isolated from the enterprise LAN. See Voice quality network requirements for more information on setting up an IP network that can support IP Telephony.

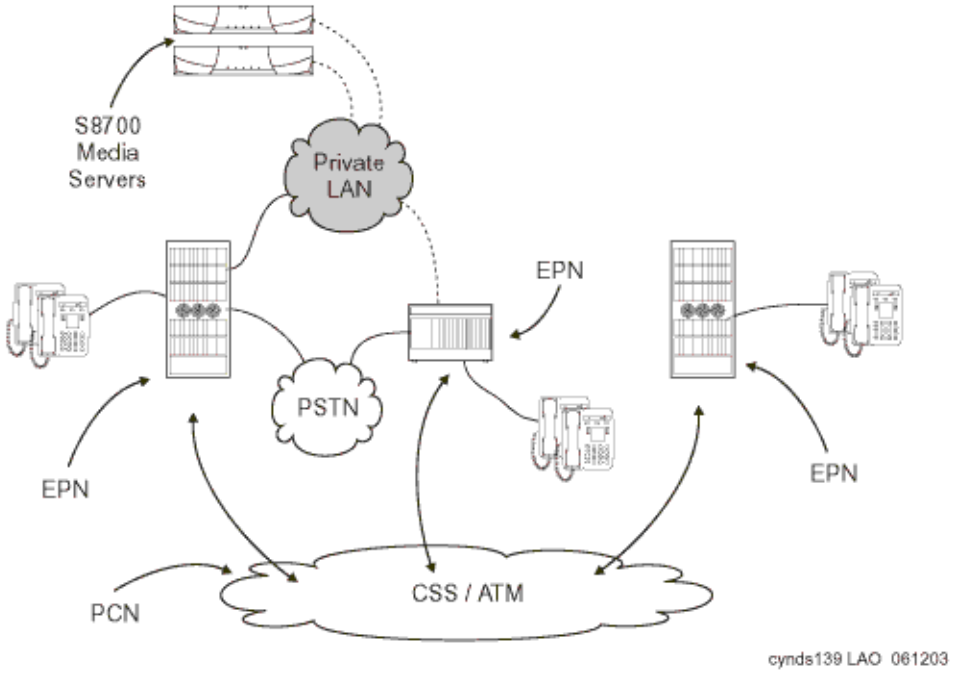
The S8700-series Server controls Media Gateways in a different manner than DEFINITY controlled Port Networks. With DEFINITY, the control path signaling shared the same transport media as the bearer channels. In a fiber-PNC system, call control signaling is established from the S8700-series Server over an Ethernet connection to the TN2312BP IP Server Interface (IPSI) in the IPSI-connected Media Gateway. Non-IPSI connected Port Networks get their control information from the servers through the Center Stage Switch to one of the Port Networks that does contain an IPSI. An IPSI can support up to five Port Networks.

The full migration from a G3r to an S8700-series Server fiber-PNC system, with traditional or ATM center stage, involves the following simplified steps:

1. Decide which EPNs are to be IPSI connected, and replace processor complexes with IPSIs.
2. Install servers.
3. Install Ethernet switches.
4. Install UPS units.
5. For IPSI-connected port networks, upgrade each EPN.
6. Connect the duplication links.
7. Connect the servers and the IPSIs to the control LAN.
8. Sequentially bring up the duplicated servers.

Figure 43: S8700-series Servers (fiber-PNC configuration) shows the completion of Phase 1, an S8700 fiber-PNC system that supports only traditional endpoints.

Figure 43: S8700-series Servers (fiber-PNC configuration)



Note:

In the traditional PBX system, signaling and bearer traffic for all calls connects through the TDM buses within Port Networks and the ATM or traditional center stage

Phase 2: IP-enable the Port Networks to support IP endpoints

Port Networks, with the addition of IP enabling circuit packs, are able to serve as Media Gateways, representing the integration of IP and TDM telephony.

IP-enabling the existing system incrementally for IP endpoint support requires the following circuit packs:

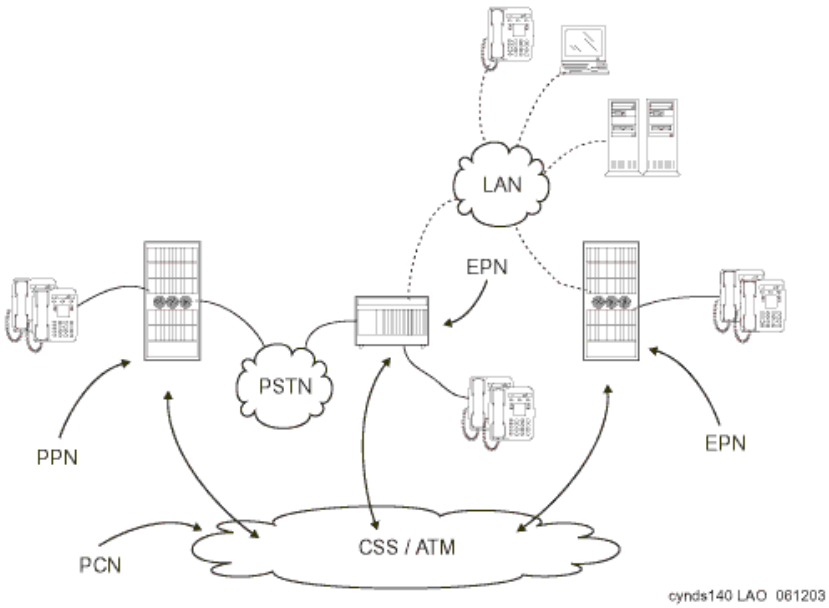
- TN799DP Control-LAN (C-LAN) for IP call signaling.
- TN2602AP IP Media Resource 320 and TN2302AP IP Media Processor for IP audio media processing, including media streams that are intended for IP Softphones and IP Telephones. Two per port network, maximum.

Signaling and bearer communication can connect through both the traditional TDM/center stage route and the IP network infrastructure. This gentle migration to IP Telephony (Figure 44: IP-enabled DEFINITY configuration) might have minimal impact on an existing, non-IP system, while simultaneously enabling all new IP endpoints to fully access all the Communication Manager features.

Note:

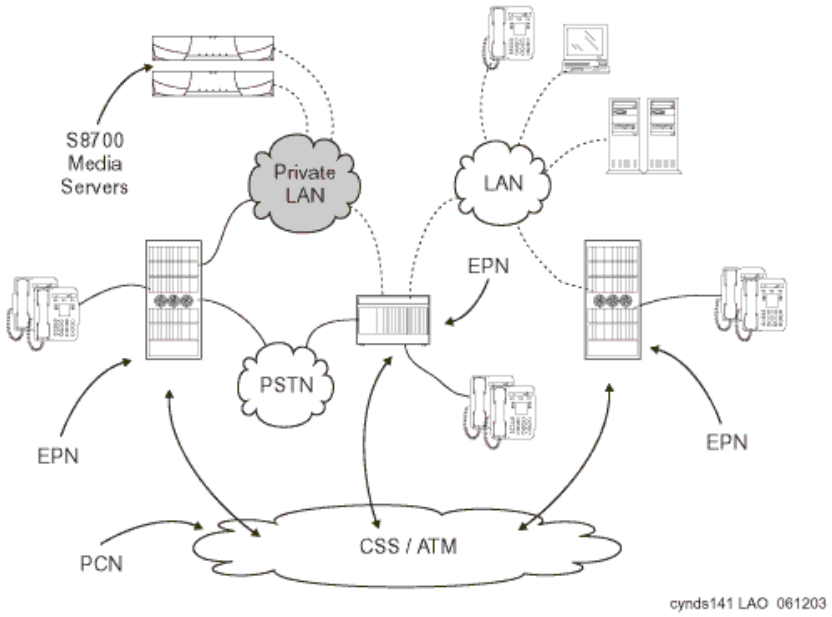
If Phase 2 is implemented before Phase 1, the system will resemble Figure 44: IP-enabled DEFINITY configuration. Also, a system that implements Phase 2 but not Phase 1 cannot support as many IP endpoints as a system that implements both Phase 1 and Phase 2.

Figure 44: IP-enabled DEFINITY configuration



At this stage, the media flow between two IP endpoints can be “shuffled.” That is, the media flow proceeds directly between both endpoints without requiring Media Processor resources. Shuffling may be used across multiple sites or multiple Avaya switches. Likewise, calls between an IP endpoint at one site and a circuit-switched endpoint at another site can be shuffled so that the media stream flows between the IP Telephone and the Media Processor circuit pack in the Port Network that is connected to the circuit-switched endpoint. By using the IP network to the greatest extent possible, enterprises can minimize the use of expensive circuit-switched trunks.

Figure 45: IP-enabling the S8700 fiber-PNC configuration

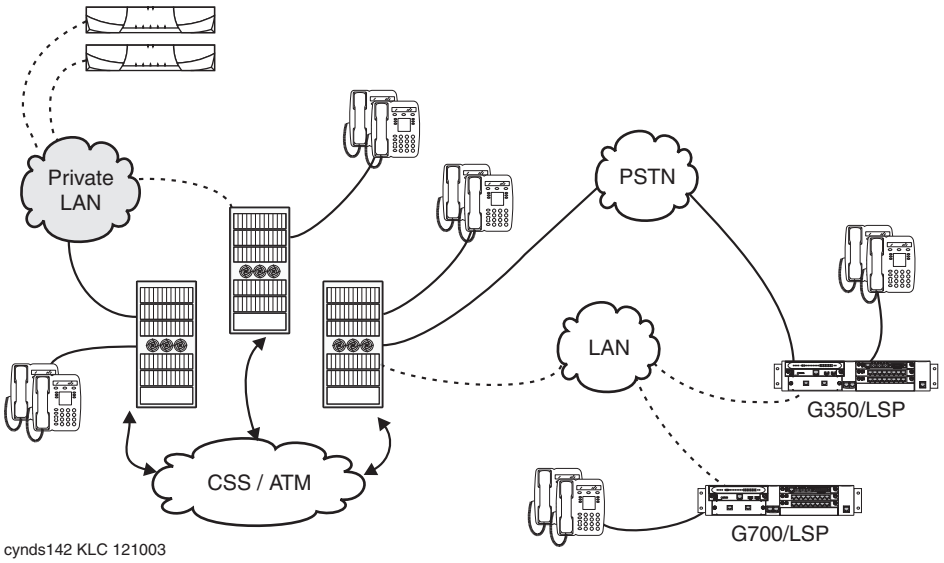


Phase 3: Server consolidation

Traditionally, some enterprises have elected to use multiple DEFINITY systems at remote sites to protect against a circuit failure on the center stage network bringing down an entire remote site. With the decision to run multiple servers came the need for additional administrative resources and a more complex dial plan. Today, through the use of IP Telephony technology and the enhanced processing capabilities of the S8700-series Servers, Avaya has a solution to consolidate smaller remote DEFINITY servers, such as ProLogix or DEFINITY ONE into an S8700 fiber-PNC system, while maintaining remote site survivability in the event of a network or processor failure. By consolidating multiple DEFINITY servers into one S8700 system, an enterprise can realize cost savings in simplified administration and a simplified dial plan. With support for up to 44,000 endpoints, the S8700-series system has the scalability to support a remote site’s server consolidation.

Consolidating remote site servers into an S8700 system requires a G700 or G350 Media Gateway with the option of Local Survivable Processors (LSP) (Figure 46: S8700 / G700 / G350 system with Local Survivable Processors). The LSP can be an S8300 or S8500 Server. In the event of a network or processor failure, the LSP takes over active call processing and gateway and endpoint management for the remote site, allowing continued operation with no loss of features until the outage is repaired.

Figure 46: S8700 / G700 / G350 system with Local Survivable Processors



Because the G700 and G350 rely on IP Telephony technology, this option is especially attractive to customers who decide to use a majority of IP endpoints at the remote site. This solution will, however, continue to support analog endpoints and DCP endpoints. Analog trunks and ISDN trunks are also supported. To decrease operational expenses, the circuit-switched trunks back to the main site can be replaced with IP trunks.

Call processing

This chapter explains the features, the strengths, and the architecture of Communication Manager call processing.This chapter emphasizes the call processing components of Communication Manager and its architecture, and briefly discusses IP-related applications in the areas of telephony, convergence, networking and call routing, mobility, telecommuting, and remote office. This chapter is not an exhaustive resource for Communication Manager features.

Communication Manager operates on the Avaya servers, and on the existing family of DEFINITY servers. Communication Manager seeks to solve business challenges by powering voice communications and integrating with value-added applications. Communication Manager provides user and system management functionality, intelligent call routing, application integration and extensibility, and Enterprise Communications networking.

For more information on Communication Manager, see:

- *Feature Description and Implementation for Avaya Communication Manager,* 555-245-205, contains details about the full capabilities of Communication Manager by release, application area, or both.
- *Overview for Avaya Communication Manager,* 03-300468, contains descriptions of each feature.
- *What's New in Avaya Communication Manager for Release 4.0*, 03-601528, provides a delta view of new features in Communication Manager Release 4.0.

  These documents are available at http://support.avaya.com.

Voice and multimedia networking

Intelligent networking and call routing

With Avaya Communication Manager, servers can use IP trunks across an IP network to communicate between switches without the need for dedicated leased lines. With Communication Manager, IP trunks can use Distributed Communication Services (DCS+) or QSIG Services to extend feature transparency, centralized voice mail, centralized attendant service, call center applications, and enhanced call routing across IP trunks.

IP Port Network / Media Gateway connectivity

IP PNC allows S8700-series Servers and G650 Media Gateways to be connected over IP networks. Avaya Communication Manager uses a proprietary method to package signaling messages over IP. This method allows deployment of communications systems throughout a customer’s data network.

H.248 Media Gateway control

Communication Manager uses the standards-based H.248 media gateway control protocol to perform call control of Avaya G700, G350, and G250 Media Gateways. H.248 defines a framework of call control signaling between the intelligent servers and multiple Media Gateways. H.248 controls both IP (H.323) and non-IP connections into a media gateway. H.248 has been extended by Avaya to also tunnel proprietary CCMS messages, to allow for enhanced call handling.

Call Processing

Communication Manager gatekeepers

A gatekeeper is an H.323 entity on the network that provides address translation and controls access to the network for H.323 endpoints. For Communication Manager platforms, these are the Avaya S8300, S8400, S8500, and S8700-series Servers. H.323 RAS (Registration, Admission, and Status) Protocol messages are exchanged between the server and the IP endpoints for the endpoint registration.

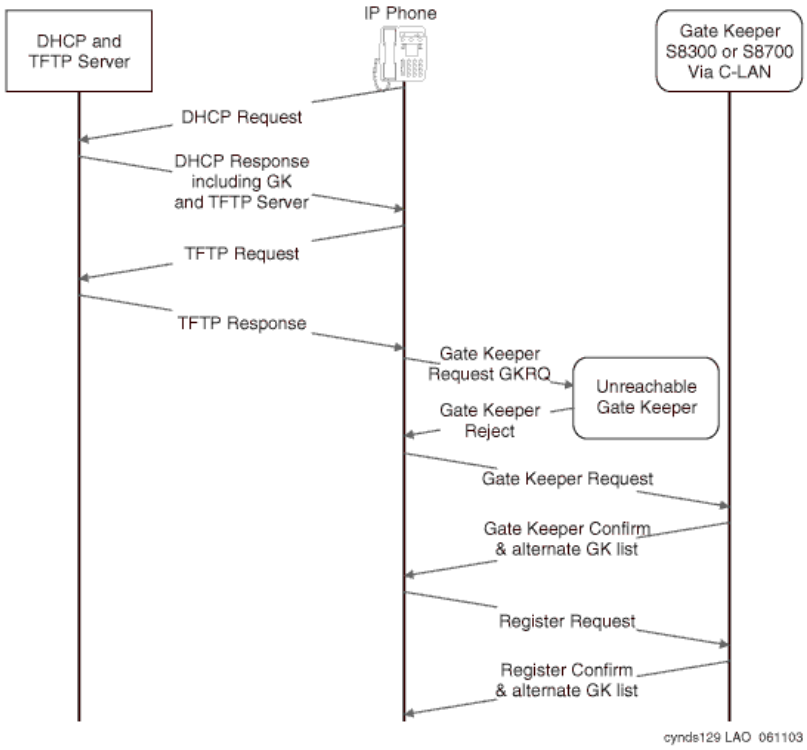
All H.323 voice applications (IP Softphones, IP agents, and IP Telephones) should register with an Avaya gatekeeper before any calls are attempted. Communication Manager sets up call signaling (Q.931) and call control (H.245) channels from endpoints to the gatekeeper. This allows Communication Manager to provide many of its calling features to H.323 calls.

Registration and alternate gatekeeper list

The RAS protocol is used by the IP endpoint to discover and register with the Communication Manager gatekeeper.

When registration with the original gatekeeper (C-LAN, S8500 or S8300) IP address is successful, the switch sends back the IP addresses of all the C-LANs (or LSPs) in the IP Telephone's network region. These addresses are used if the call signaling to the original C-LAN circuit pack fails. Figure 47: Discovery and registration process to the gatekeeper on page 128 shows the registration process.

Figure 47: Discovery and registration process to the gatekeeper



Call signaling

Communication Manager implements the gatekeeper routed call model of H.323. The registration process that is described above allows the endpoint and the Communication Manager gatekeeper to exchange addresses to establish a TCP connection for a “call signaling” channel (the H.323/H.225 channel). Once the TCP connection is established for call signaling, the H.225.0/Q.931 signaling protocol is used over that connection to route the call and exchange addresses necessary to establish a second TCP connection. This second TCP connection is used for “media control” (the H.245 channel).

When Communication Manager chooses to route the media flow streams through the switch, it selects and allocates available media processor resources, and sets the corresponding circuit packs up to receive and send the media stream or streams from/to the endpoints using the negotiated capabilities for each terminal. Each terminal is told to send its media stream or streams to the appropriate Media Processor circuit pack. The switch connects the two media streams, and thus completes the bearer path between the terminals.

Media stream handling

Media processor circuit packs (VoIP resources)

The basic functions of the TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit packs, and VoIP on the G700/G350 Media Gateways, include:

- Taking media streams off the IP network, terminating RTP/UDP (adjusting for variable delay in arrival rate), and converting them into PCM audio for transmission on the TDM bus.
- Taking media streams from the TDM bus, encoding them with the proper codec, and transmitting them as RTP packets to an IP endpoint.
- Originating and terminating an RTCP control channel for each media stream.
- Encryption and decryption of media

The particulars of the media conversion that is to be performed on each media stream are controlled by Communication Manager. The Quality of Service (QoS) information obtained from the RTCP channel is passed from the circuit pack to Communication Manager.

DTMF tone handling

The Media Processor circuit pack listens for and detects DTMF tones coming from the TDM bus, strips them out of the audio stream, and sends a message to the server indicating that it has done so. The server in turn generates and sends the appropriate H.245 tone message to the endpoint that is receiving the audio stream. The receiving endpoint then plays the specified tone. Compressed codecs, such as G.729, generally do a poor job of passing DTMF tones. By sending tones out of band, fidelity is maintained. This method is useful when connecting to a voice mail or an integrated voice response (IVR) system, where DTMF digits are used to navigate through prompts.

When this capability is used on an H.323 tie trunk between Communication Manager switches, the switch that receives the H.245 tone message plays the required tone onto all the ports receiving the audio stream.

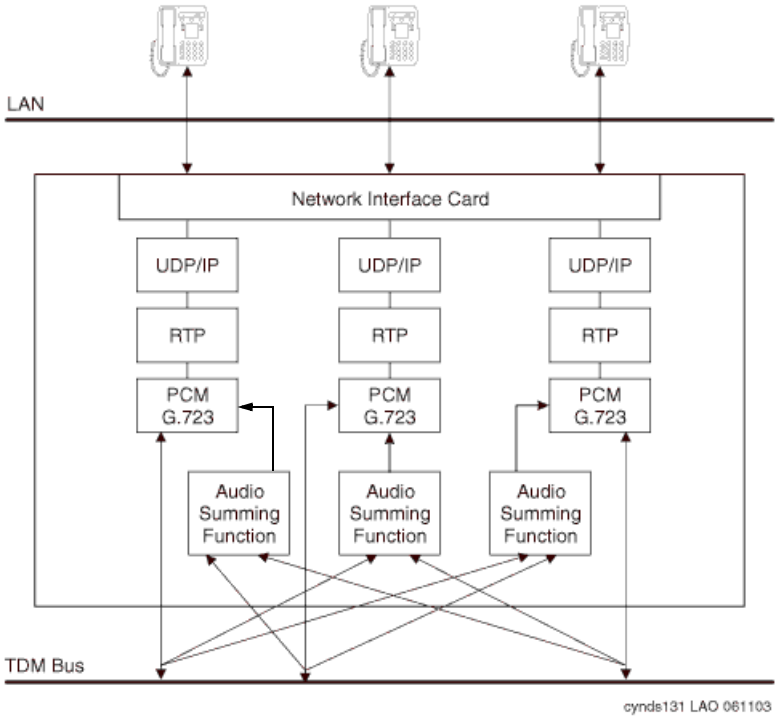
Media stream for audio conferencing

When calls between IP endpoints are conferenced, the media streams must be routed through the Media Processor board

Communication Manager allows the audio streams from different parties to come into different Media Processor circuit packs. Each Media Processor sends its received signal to the TDM bus in Pulse Code Modulation (PCM) format. All the other processors serving endpoints on the call can then receive and sum the audio signals coming from all parties, and send the resultant composite audio stream to the IP parties that it supports.

Figure 48: Media Processor board support of a three-party audio conference on page 130 provides an example to show how the Media Processor board is configured for a three-party H.323 audio conference using G.729. This conference is conventional in that it uses TDM bus timeslots to allow each party to listen to all of the other parties. However, a more efficient form of conferencing is possible when all the parties are IP endpoints, where the audio streams are multiplexed directly on the Media Processor circuit pack, and no TDM timeslots are used. To establish the configuration shown in Figure 48: Media Processor board support of a three-party audio conference on page 130, the DSP resources on the Media Processor board are allocated as needed to audio conferencing. Communication Manager balances the available media processing resources, effectively sharing load among multiple Media Processor boards.

Figure 48: Media Processor board support of a three-party audio conference



Separation of Bearer and Signaling (SBS)

In an Avaya IP Telephony system, call signaling and bearer traffic may be routed over separate paths. This is useful for a remote branch office with only limited WAN bandwidth back to headquarters. Call signaling traffic can be routed across the WAN, while bearer traffic is sent over the PSTN.

Multi-location

Communication Manager release 2.2 or later allows a Linux-based server located in one country to control gateways located across national borders and provide appropriate country-specific tones and features. Specifically, these features include the following:

- A-law & Mu-law Companding
- Call Progress Tone Generation
- Loss Plan
- Analog line board parameters
- Call Detail Recording
- R2-MFC (Multifrequency-Signaling) trunks

Multi-location functionality is subject to the following limitations:

- 25 Countries
- R2-MFC: 8 signaling sets
- Additional Tone Generators (TN 2182 in Port Networks, built-in tone generators in Media Gateways) are required to support country-specific tones
- No per-country alarms or traffic reports are available
- LSPs must be set to the same time zone as the server
- This feature is intended for IP-remoted gateways, not DS1-remoted Port Networks.

Modem/Fax/TTY over IP

In the past, many organizations have experienced problems transporting modem, fax, and TTY tones over an IP Telephony network, regardless of vendor. Modems, faxes, and TTYs are very sensitive to latency and jitter, and do not tolerate distortion induced through compression, expansion, and transcoding. In order to overcome these difficulties, Avaya has enhanced its modem, fax, and TTY-over-IP support in release 2.2 and later.

There are two enhanced modes for supporting Modem-over-IP (MoIP): pass-through and relay. Pass-through is essentially a best-effort transmission, and works by forcing the use of the G.711 (uncompressed) codec for the call. Re-transmission is governed by the application. Pass-through mode is suited to LAN environments where both ends of a call are synchronized using a common clock source. Relay, on the other hand, uses redundant packet transmission to protect against packet loss. Because relay mode does not force the use of G.711, it requires less bandwidth than pass-through, however requires more DSP resources. Relay is more effective than pass-through across a WAN.

Avaya's TTYoIP support works by identifying TTY Baudot tones at the near-end Media Processor, removing them from the voice path, and transporting them across the network in RFC 2833 messages. The far-end Media Processor receives the RFC 2833 messages and regenerates them for the far-end station. This feature is enabled by default on IP trunks and inter-gateway calls, and is capable of toggling between text and voice modes.

Avaya's support for modem, fax, and TTY over IP can be summarized as follows:

- TTY over IP continues to be supported
- Modem Pass-through is supported between Avaya gateways
- Modem Relay at 9.6K is supported between Avaya gateways
- Avaya supports sending multiple instances of the same packet

Redundant transmission mitigates the effects of packet loss, but requires additional bandwidth.

Avaya's modem, fax, and TTY over IP support is subject to the following limitations:

- QOS is required, even on LAN.
- Avoid MoIP where possible (especially over a WAN environment)
- Use circuit-based resources on the same gateway
- Use different classes of service and restrictions
- Use centralized modem pooling for larger communities
- Only one TDM-to-IP-to-TDM conversion is allowed
- Send duplicate streams, where practical

Table 3 summarizes Avaya's fax, modem, and TTY options.

Table 16: Fax, Modem, and TTYoIP options

Fax	**relay**	Default, Avaya-proprietary mode, interoperates with previous releases
	Pass-thru	Proprietary mode; uses more bandwidth, fewer DSP resources
	off	system ignores fax tones, call remains in administered codec
Modem	**off**	Default, system ignores modem tones, call remains in administered codec
	relay	Avaya-proprietary mode, most reliable modem-over-IP mode
	pass-thru	similar to Fax pass-thru
		1 of 2

Table 16: Fax, Modem, and TTYoIP options (continued)

TTY	**US**	Default, 45.45 Baudot, interoperates with previous releases
	UK	50 Baudot
	pass-thru	similar to Fax pass-thru
	off	system ignores TTY tones, call remains in administered codec
		2 of 2

IP-based trunks

In circuit switched networks, trunks provide the means to interconnect PBXs with each other and to the PSTN. Connection to the public network allows PBX station users to call and be called by terminals that are not part of the PBX private network. An analogous arrangement exists in packet-switched IP networks.

H.323 trunks connect H.323 systems or gateways over IP networks, similar to circuit-switched tie trunks. Similarly, SIP trunks connect SIP systems or gateways over IP networks.

A set of Communication Manager switches can each be attached to an IP network, and voice and fax calls can flow between them in the usual manner except that the call signaling and audio/fax streams are carried over the IP network. The signaling is carried through the C-LAN circuit packs, and the audio and fax streams are carried between switches through the Media Processor circuit packs.

The benefits of using IP trunks include:

- Reducing long distance voice and fax expenses
- Facilitating global communications
- Providing a fully functional network with data and voice
- Converging and optimizing networks by using the available network resources

IP trunk calls can be compressed to save network bandwidth. Repeated compression and decompression (transcoding) results in a loss of data at each stage and degrades the final quality of the signal. The maximum recommended number of compression cycles on a call is three. Normal corporate voice calls or fax calls typically go through fewer than three compression cycles.

IP (H.323 and SIP) trunks can also connect to other vendors' compliant PBXs.

IP tie trunks

IP tie trunks are used to connect switches to one another. When an IP trunk is used to interconnect two switches, the trunk can also carry standard (QSIG) and proprietary (DCS+) signaling for interswitch feature transparency. The location of each other node (switch) in the network is administered, and node selection is based on the dial plan and call routing features such as AAR/ARS.

H.323 or SIP tie trunks are administered as a new type of trunk group. Instead of administering ports as members of the trunk group, only the number of channels must be specified. Each channel is analogous to a member trunk. In addition, an IP tie trunk can be made a member of a signaling group so that a virtual D-channel can be administered and used to carry feature transparency information.

For SIP trunk capacities, see Table 17: SIP Trunk Capacities by Platform Configuration on page 135.

Trunk signaling

Several variations of IP signaling must be accommodated for the variety of trunks supported by Communication Manager. These are specified as options in the trunk group administration. When the IP trunk is used as a tie trunk to another vendor's switch, gateway, or gatekeeper, Communication Manager sets up a separate TCP connection for each call.

Note:

As of Communication Manager release 3.1, the maximum number of members of a single IP trunk signaling group has increased from 31 to 255.

For more on trunk signaling, see *Overview for Avaya Communication Manager,* 03-300468.

SIP

SIP stands for Session Initiation Protocol, an endpoint-oriented messaging standard defined by the Internet Engineering Task Force (IETF). SIP is a text-based protocol, similar to HTTP and SMTP, for initiating interactive communication sessions between users. Such sessions include voice, video, instant messaging, interactive games, and virtual reality.

SIP "trunking" functionality is available on any of the Linux-based servers (S8300, S8400, S8500, or S8700-series). SIP trunking allows Avaya Communication Manager to communicate with SIP endpoints and gateways across an IP network. SIP trunks allows an enterprise to connect its server(s) to a SIP-enabled proxy server, specifically, an Avaya SIP-Enablement Server (SES), and through this proxy, optionally to an external SIP service provider, if desired. The trunk support in Communication Manager complies with SIP standards, specifically IETF

RFC 3261, and so interoperates with any SIP-enabled endpoint/station that also complies with the standard.

Table 17 shows the maximum number of SIP trunks supported out of the total number of IP trunks supported.

Table 17: SIP Trunk Capacities by Platform Configuration

Platform Configuration	Maximum Number of SIP IP Trunks of the Total IP Trunks Supported
S8700-series (fiber-PNC or IP-PNC)	5000 of 8000
S8500	800 of 800
S8400	400 of 400
S8300/G700/G350	450 of 450
S8300/G250	10 of 10

Avaya Communication Manager supports SIP endpoints, including the Avaya 4602 SIP Telephone and Avaya IP Softphone Release 5. In addition to its IP telephony capabilities, IP Softphone R5 also includes Instant Messaging (IM) client software, which is a SIP-enabled application that connects to the Avaya Converged Communication Server for IM control. By means of having SIP-enabled endpoints managed by Communication Manager, many features can be extended to these endpoints. The servers (S8300, S8500 or S8700-series) function in four ways:

- As Plain Old Telephone Service (POTS) gateways
- As support for name and number delivery between and among the various non-SIP endpoints supported by Communication Manager

  For instance, analog, DCP (Digital Communications Protocol) or H.323 stations, and analog, digital or IP (internet protocol) trunks.
- As support for new SIP-enabled endpoints, such as the Avaya 4602 SIP telephone
- As a telephony feature server to SIP endpoints

  The set of features supported by SIP itself is augmented by those supported by Communication Manager.

Avaya SIP Enablement Services (SES)

Avaya SIP Enablement Services (SES) is part of the Converged Communications Server portfolio with Application Enablement Services (AES). Prior to SES 3.0, SES was named Converged Communications Server as a product name, but that was later made a portfolio-level

name. As of SES 4.0, there is no integration between AES and SES, and the Converged Communications Server portfolio is a marketing name.

Overview

SES is sold as a communications appliance similar to Avaya Communication Manager, and is deployed on the X305 (3.0, 3.1) and X306 and X306M IBM Servers since 3.1.1. The main functions of SES are to provide SIP networking capabilities and support SIP endpoints in a converged communications network. SES supports multiple SIP standards as well as Avaya value-add services and features that are not defined in the standards.

The main processes on SES are a SIP proxy server, SIP registrar, SIP Event and Presence Server, profile services, and a built-in centralized administration system for all SES servers in a network. Additionally, there is a centralized trace logger, IM logger, SIP conferencing server (used with Communication Manager) and a robust high availability platform for supporting duplicated servers and the SAMP daughter board for remote maintenance purposes.

The SES Server

The SES server is composed of the following components:

- SIP Proxy Server and Registrar
- SIP Event Server (includes Presence and other event packages)
- SIP Conference Manager (implements SIPPING standards)
- Personal Profile Manager (PPM) web service
- SIP Personal Information Manager (SPIM), end user web interface for profile management
- SES Master Admin System - centralized administration for all SES servers
- SES Administrative Web Services
  - Master Admin Web Service (MAWS)
  - Home Admin Web Service (HAWS)
- SES High Availability Platform
  - Duplicated Server Support
  - SAMP
  - Watchdog
  - Alarming
  - Logging
- SES Trace Logger - centralized trace logger for all SES servers
- IM Logger - IM logging capability administered per node
- SES Database

The high level architecture is a shared data approach, where most components do not interact directly with each other, but rather all share and use data in the database. The master admin system populates that data from a single web interface, and run-time components read and modify that data. In some cases, there are specific interfaces between components: the event server is reached through the proxy using SIP, the event server and PPM use a SOAP service for profile notifications, and the trace logger communicates between the proxy's logging capabilities and MAWS.

The SES Network

As a proxy infrastructure, SES is at the heart of SIP communications, routing messages between other SIP networks, SIP feature servers, SIP adjuncts, and SIP endpoints in the SIP network. Two terms describe an SES server: Edge Server and Home Server. An "Edge Server" communicates with external SIP networks, and a "Home Server" provides service to endpoints. The most basic server is a single-box solution that provides both Edge and Home capabilities and is referred to as a Home-Edge server. The Home-Edge server contains all of the SES components, can be configured to route to external domains, and provides service to SIP endpoints.

SES Edge Server

The SES Edge Server provides routing to external domains as well as hosting the global routing table for the enterprise. While it does not have specific knowledge of SIP endpoint registrations, it knows where users are on the network. In fact, it knows where to route each SIP address in that domain.

The SES Master Admin system is resident on the edge server.

SES Core Router

The SES Core Router is an enhancement to the Edge Server to perform prefix-based routing between branches in the Distributed Office environment.

SES Home Server

The SES Home Server provides service to SIP endpoints. The Home Server routes the Advanced SIP Telephony (AST) capability with Communication Manager, provides a SIP registrar, and contains the Personal Profile Manager web service and end-user web interface for profile management.

Communication Manager as the SIP Feature Server

Communication Manager implements SIP trunk and the Advanced SIP Telephony (AST) feature set utilizing OPTIM capabilities in Communication Manager. This allows a SIP endpoint to signal

feature using Feature Name URIs, and retrieving state through event packages. Advanced SIP users must be provisioned both on SES as a SIP user and as an OPTIM station on Communication Manager. There must be a SIP trunk configured on Communication Manager, and a corresponding server configured on SES.

For AST, calls will be routed through Communication Manager for feature processing in both originating and terminating features.

Non-SIP endpoints can be dialed from SIP endpoints (and vice versa) by having server address maps on SES.

SIP Adjuncts

The first SIP adjunct supported was Modular Messaging, where message waiting indicator (MWI) and message retrieval are provided via SIP. In SES 4.0, Voice Portal support was added. Additionally, the development teams for Communication Process Manager (CPM) and Meeting Exchange Express Version are performing interoperability testing with SES.

SIP Endpoints

Table 18: SIP Endpoints

Endpoint	Features
4602	Basic SIP phone, voice, no IM or presence
4610	Basic SIP phone, voice, no IM or presence
4620	Basic SIP phone, voice, no IM or presence
Avaya IP Softphone R5	H.323 voice, SIP IM and presence
Avaya one-X Mobile Edition (SIP Softphone)	SIP voice, IM, Presence, advanced profile features
Avaya one-X Deskphone SIP (9620,9630)	Advanced SIP telephony, advanced profile features, IM/Presence
Toshiba SIP Phone	Advanced SIP telephony, advanced profile features, no IM/Presence

In addition to the endpoints listed, other third party endpoints are supported though the Avaya Solution Interoperability Lab.

SIP deployment scenarios

SIP and DNS

In all SIP configurations it is highly recommended to use both Dynamic Name System (DNS) and Dynamic Host Configuration Protocol (DHCP). The customer must have DNS running in the enterprise for external lookups. Proper DNS configuration allows for proper server resolution, including external domains, as well as ease of provisioning within the intranet. The SIP domain is used for addressing at the SIP level, such as sending an invite to user1@avaya.com. DNS is used for looking up individual host addresses in a network. This allows a SIP user to move around the SIP network, registering at different locations in the IP network, and even using different phones, while maintaining a common public address – e.g. user1@avaya.com.

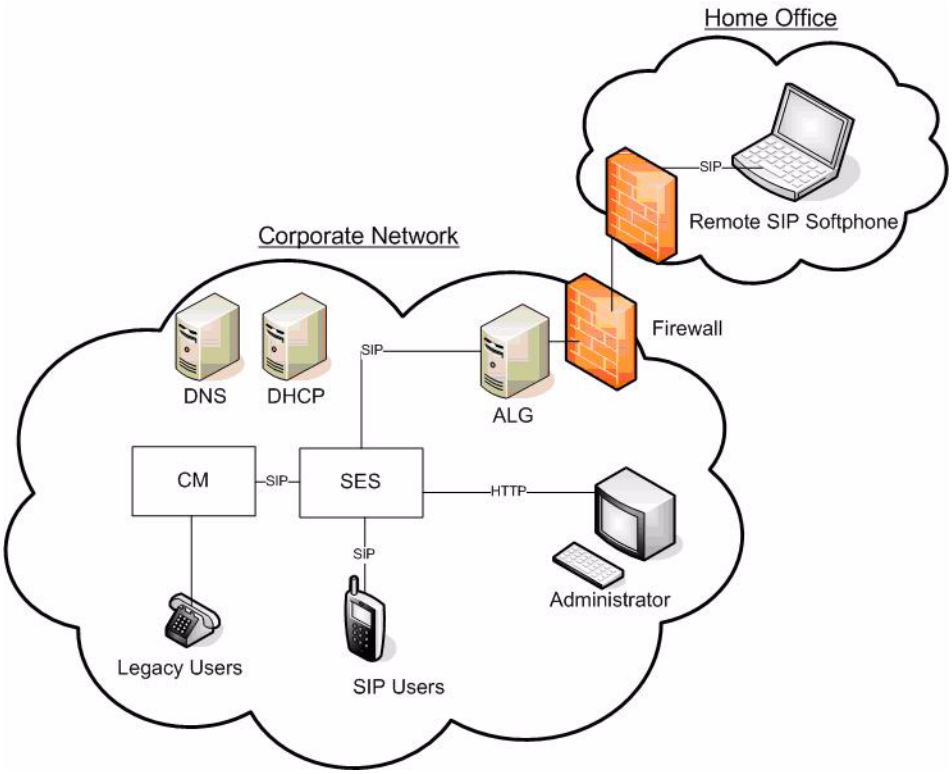
SES only supports a single SIP domain in a deployment. This domain is usually the top level domain for that enterprise, e.g. avaya.com. Often people reference the cs.columbia.edu configuration which at first glance looks like a sub-domain of columbia.edu. From the SES perspective, configuring a system like cs.columbia.edu and columbia.edu would be two separate domains and each one would view the other as an external domain. Each system would be viewed like any other deployment, having it's own administration, users, etc.

Home-edge single box solution

SES is available as a single box solution in any of the releases. The home/edge system is the most straightforward configuration and includes configuration of surrounding services for proper operation. An Access Layer Gateway (ALG) is required for traversing the firewall. SIP capable ALGs are required to handle the appropriate ports/address translation needed for SIP signaling and RTP media.

Figure 49: Typical home/edge configuration on page 140 shows a typical home/edge configuration which is valid for any release. Additionally a remote-end user using a VPN tunnel is shown. While SES may support TLS, TCP and UDP as transport protocols, the use of Transport Layer Security (TLS) is recommended whenever possible. The 2.0 and 2.1 releases include presence between Softphone clients, but no subscriptions to Communication Manager extensions and no presence server. The 3.0 release includes the presence server for additional presence features and policy management.

Figure 49: Typical home/edge configuration



Multi-home multi-Communication Manager system

The multi-home system is a distributed version of the home/edge system where the edge is a separate host from the home servers, which are deployed for the user base. The home servers provide service to endpoints and are associated with one or more Communication Manager hosts. The ethernet topology is orthogonal to the SIP topology. There are no restrictions or requirements on the network beyond existing preferred network setup for VOIP. The only area where SIP is concerned is access to external domains. Figure 50: Multi-home multi-Communication Manager configuration on page 141 shows an ALG between the Edge node and the service-provider cloud.

The ALG and/or the Edge node may be deployed in the customer's DMZ if they so wish. The multi-home distributed network provides scalability through user distribution, i.e. a user has only one home. To increase the size of the entire system, more home nodes are added until the edge reaches maximum capacity. Any calls that are not to a user local to the home of the originating caller are routed through the edge node.

Starting in release 2.1, any SES node on the network may be a duplicated system. There are no constraints on which nodes must be duplicated. For example, the edge and one home may be duplicated systems and the others may not be; it makes no difference because the node is one logical entity.

Figure 50: Multi-home multi-Communication Manager configuration

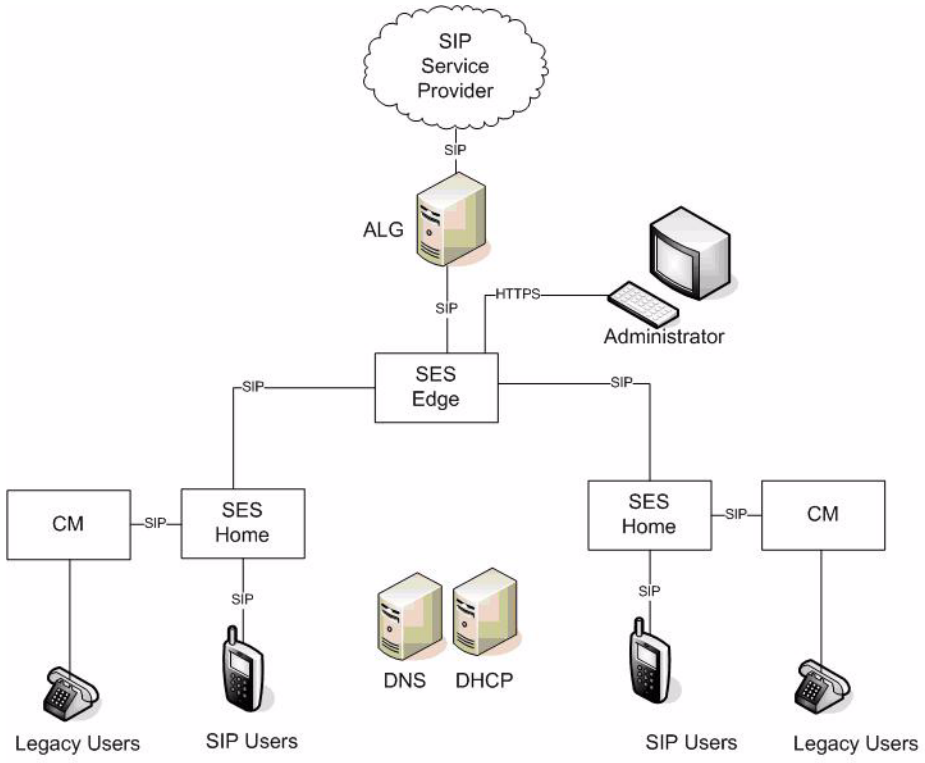
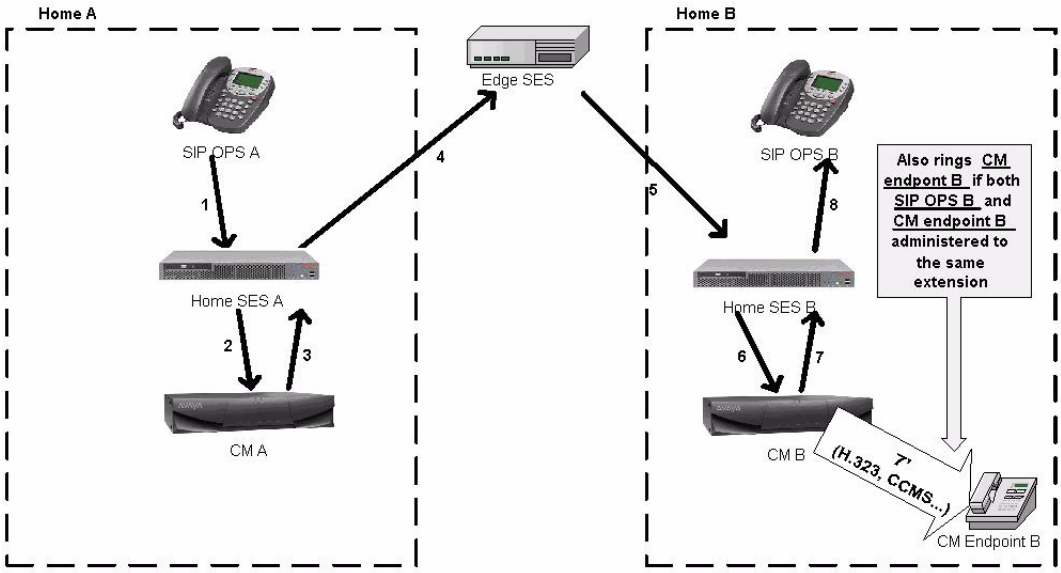


Figure 51: Message flow for multi-home multi-Communication Manager configuration on page 142 shows the message flow, where the arrows in numerical order represent the path of the initial INVITE message starting from the caller. Messages starting from the receiving station (B) travel in the exact opposite sequence.

Figure 51: Message flow for multi-home multi-Communication Manager configuration



Multi-home single Communication Manager system

One possible configuration is to only have a single Communication Manager system in the SIP deployment. The reason for doing this is to support features where SIP/AST users must located on the same Communication Manager system for certain features. One of these scenarios is the bridging feature in Advanced SIP Telephony (AST). For Communication Manager to properly handle the bridging notifications and feature interactions, the bridged users must be on the same Communication Manager system.

This configuration has a particular optimization: instead of routing a call through the edge for home-to-home calls for two SIP/AST users, Communication Manager will send the call to the far-end home after the origination processing is complete. For example, say Al is located on the Lincroft SES, and Duffy is located on the Denver SES. When Al calls Duffy, AST does originating processing for Al and realizes that Al is calling another OPTIM user on the same system, and then sends it to the home for that user (see Figure 53: Multi-home single Communication Manager configuration - message flow on page 143). This means in this configuration, the edge would be used purely for out-of-domain calling.

Figure 52: Multi-home single Communication Manager configuration

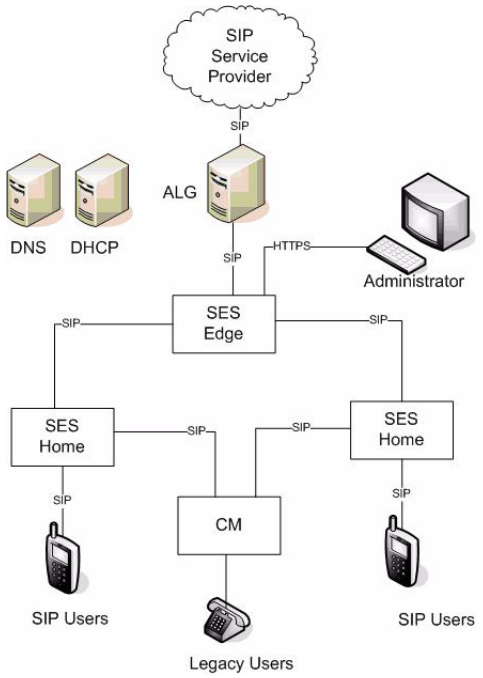
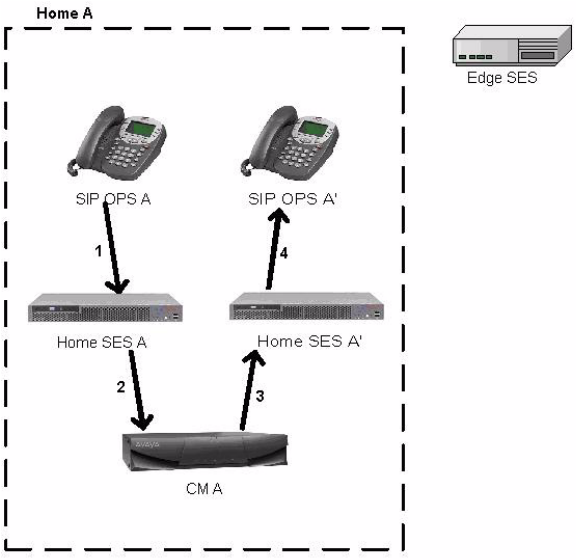


Figure 53: Multi-home single Communication Manager configuration - message flow



Multi-home multi-Communication Manager with QSIG (TIE trunk) connection

An alternative to the single Communication Manager configuration is to have one logical Communication Manager system, but have two Communication Manager servers connected with QSIG or standard Communication Manager TIE trunk connection using ISDN or IP trunks. This increases the total capacity of the solution and retains the optimization of having only one Communication Manager system with multiple SES home servers. Customers with existing systems of Communication Manager servers would likely have the QSIG infrastructure already in place before they upgrade to SIP.

Figure 54: Multi-home multi-Communication Manager configuration with QSIG connection

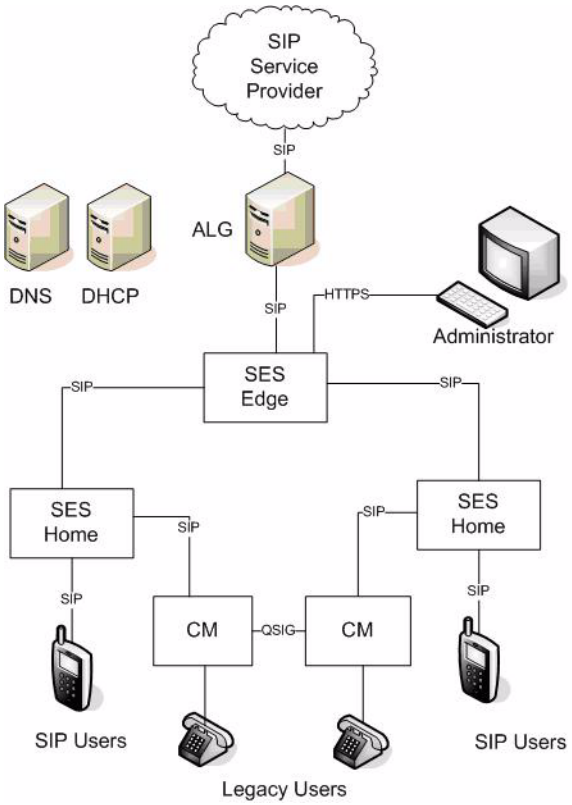
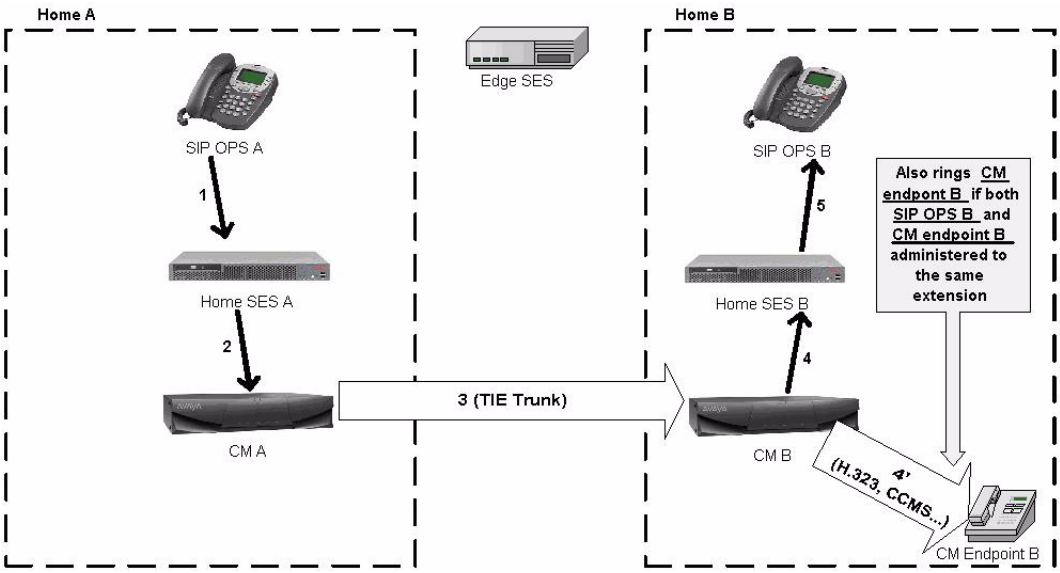


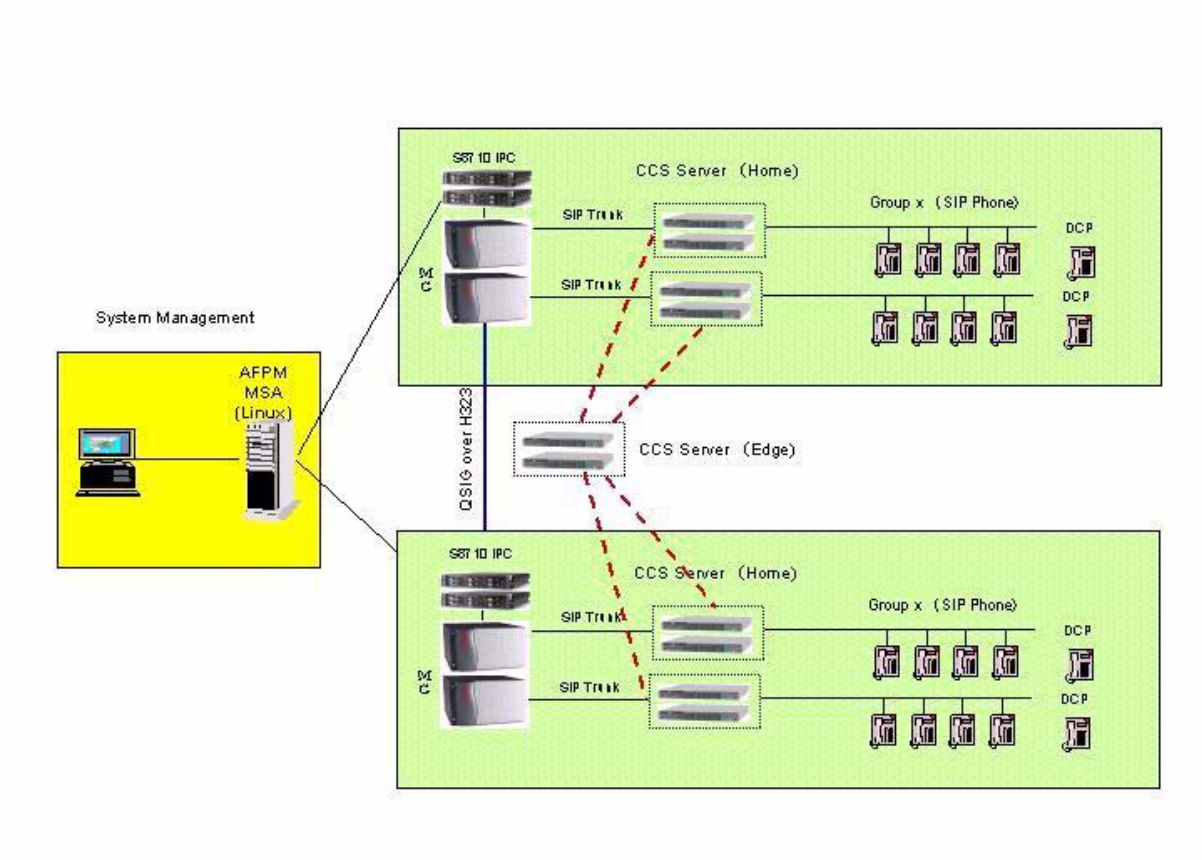
Figure 55: Multi-home multi-Communication Manager configuration with QSIG connection - message flow



Avaya-Toshiba Solution

Avaya and Toshiba have collaborated to provide a combined Avaya AST solution (Communication Manager and SES) with Toshiba SIP terminals for the Japanese general office market. Development and testing are specifically targeted to the unique Japanese market where each DID phone number is used to reach a group of people, called the "workgroup." The workgroup may be an individual (executive) or a group of workers (for example, accounting). The average number of members in a group is about 5. Calls to the DID number results in SIP NOTIFY messages sent to each member of the workgroup.

Figure 56: Avaya-Toshiba Solution



Avaya G860 Media Gateway

The Avaya G860 media gateway is a DS3-capable, high channel density standards-compliant, VoIP media gateway system. It provides a robust, scalable, and modular solution designed for a large campus or call center with high availability and reliability. To support high availability, the Avaya G860 Media Gateway features automatic protection switching and full redundancy of all common equipment.

G860 is a high capacity, cost-effective IP telephony trunking system that supports up to four T3s (redundant 3+1 media gateway board configuration). The media gateway supports SIP for interoperability with a wide range of communications applications.

G860 features include:

- G860 support up to 5000 voice channels in Avaya Communication Manager Configuration
- Supports multiple DS3s
- Redundant power supply units, System controller, Ethernet switch
- Optional N+1 media gateway boards
- Scalable density options
- Open, scalable SIP-based architecture

Figure 57 and Figure 58 show the front and back views, respectively, of the G860 Media Gateway.

Figure 57: G860 Front view

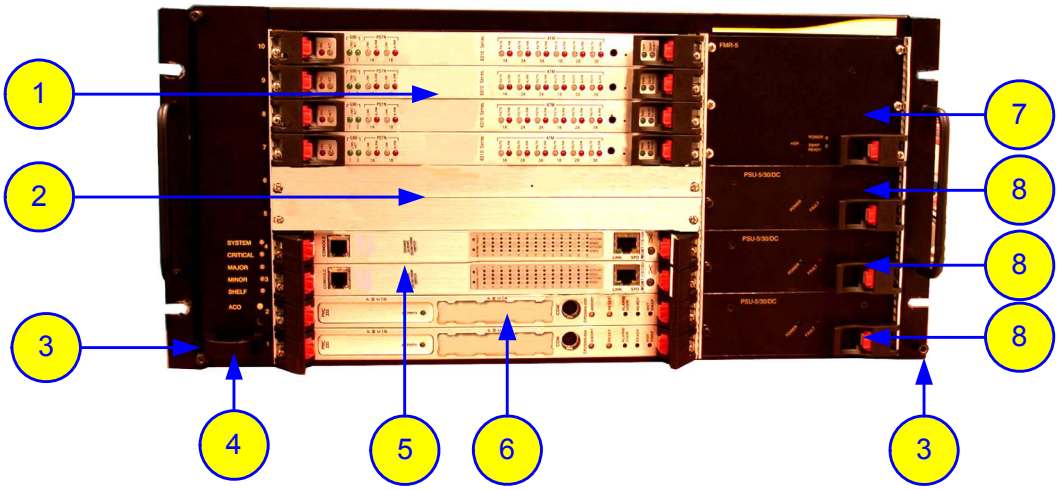


Figure notes:

1. Trunk Processing Module (TPM) boards
2. Blank and baffled panels
3. ESD connectors on the attachment brackets
4. Fan Tray Module (FTM) with alarm LEDs
5. ES 6600 Ethernet switch boards
6. System controller (SC) boards
7. FMR Auxiliary fan module
8. Power supplies

Figure 58: G860 Back view

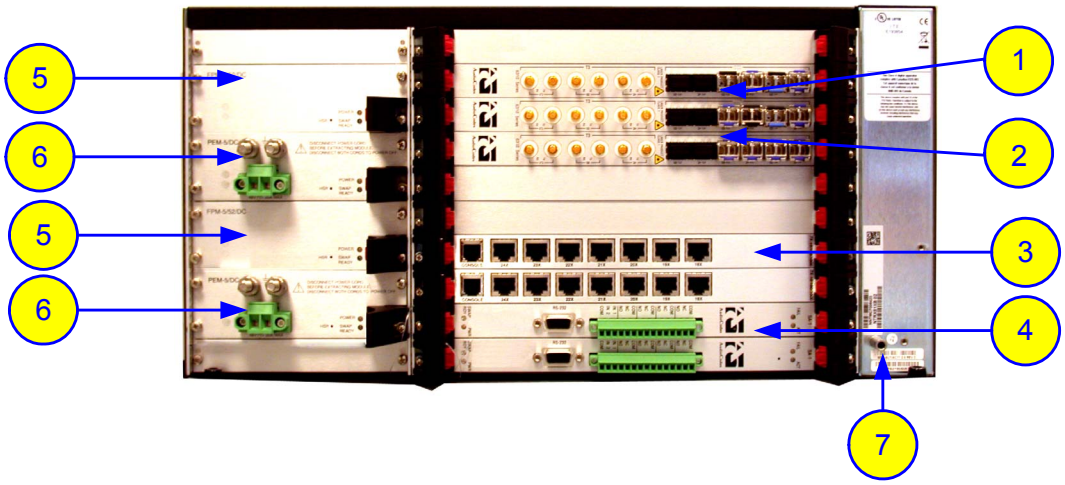


Figure notes:

1. TPM I/O Rear Transition Module (TPM/RTM/Redundant)
2. TPM/RTM
3. ES/6600/RTM
4. SA/RTMs
5. PEM units
6. FPM advanced fan module
7. ESD connections

G860 Components

The G860 media gateway hardware consists of the chassis, TP6310 (media gateway board), Ethernet Switch, System Controller, and the corresponding Rear Transition Modules (RTM).

Table 19 lists the G860 Media Gateway components and redundancy configuration.

Table 19: G860 Media Gateway components

Component	Redundant Configuration
Chassis	1
System Controller (SC)	2
Synchronization and Alarm Rear Transition Module (SA/RTM)	2
Ethernet Switch Board – 24 Gb (ES/6600)	2
Ethernet Switch 7 I/O Rear Transition Module (ES/6600/RTM)	2
Trunk Processing Module media gateway Boards	Up to 4
TPM I/O Rear Transition Module (TPM/RTM)	Up to 3
TPM I/O Rear Transition Module – Redundant (TPM/RTM/HA/Redundant)	1
DC Power Supply Modules (PS/DC or PS/AC)	3
DC Power Entry Modules (PEM/DC or PEM/AC)	2
Fan Tray Module (FM)	
Air Filter (AF)	1
Auxiliary Fan Tray Module (FMR)	1
DC Fan Tray Power Supply Module (FPM)	2
Blank Panels (Full Configuration): Blank panel — Panel only Blank panel — Baffled filler panel	 1 1

System Controller Board

The G860 contains two System Controller (SC) boards, which control and monitor the G860 media gateway operation. The SC boards are installed into their dedicated slots. Each controller

contains an on-board hard disk, which stores the SC software and the configuration and performance database.

The SC board incorporates a 650 Mhz UltraSparc processor with 512 MB memory and uses the robust Solaris operating system environment enhanced for advanced high-availability features. The SC board is designed in compliance with the PICMG CompactPCI standards for high-availability systems. It supports hot-swap operation, system management, and environmental monitoring.

Two 10/100 Base-TX redundant Ethernet ports connect the SC boards with two Ethernet Switch boards. Each SC board is accompanied by a Synchronization and Alarm (SA) Rear Transition Module (RTM) board.

G860 Trunk Media Processing Module (TP-6310)

The G860 Trunk Processing Module (TP-6310) is a high-density, hot-swappable, compactPCI resource board with a capacity of 672 DS0 channels, supporting all necessary functions for voice, data, and fax streaming over IP networks. TP-6310 provides STM-1/OC-3 (future), PSTN, ATM, and T3 interfaces via its Rear transition Module (RTM).

Slots 7 to 10 of the G860 chassis are used for up to 4 trunk processing modules (including the redundant TP-6310) according to customer requirements. The PSTN interface and the ATM interfaces are provided with 1+1 protection.

For redundant N+1 protection, the 6310/RTM/HA/Redundant Standby board is provided. It contains no port connection and occupies slot 10.

Note:

The Trunk Processing Module is hot-swappable for redundant systems. However, the board must be locked in order to be replaced, which takes the board out of service.

Configuration with Avaya Communication Manager

Avaya G860 Media Gateway provides SIP connectivity to Avaya Communication Manager and can work in conjunction with the G650 Media Gateway. This solution is ideal for Large IP-based contact Centers and Campuses.

The G860 with Avaya Communication Manager provides non blocking SIP-VoIP capacity of up to 5000 channels. In this configuration the G860 eliminates the need for T1/E1 resources by providing multiple DS3, where each DS3 is equivalent to 28 DS1 interfaces.

In this configuration, the following boards are needed according to enterprise traffic.

- C-LAN — for the signaling links between an Avaya Linux based server and SIP Adjuncts such as SES, G860, and Expanded Meet-me conference bridge
- IPSI — for signaling between the Linux based servers and other Avaya media gateways.
- Media Processor resource board — for calls that do not shuffle.

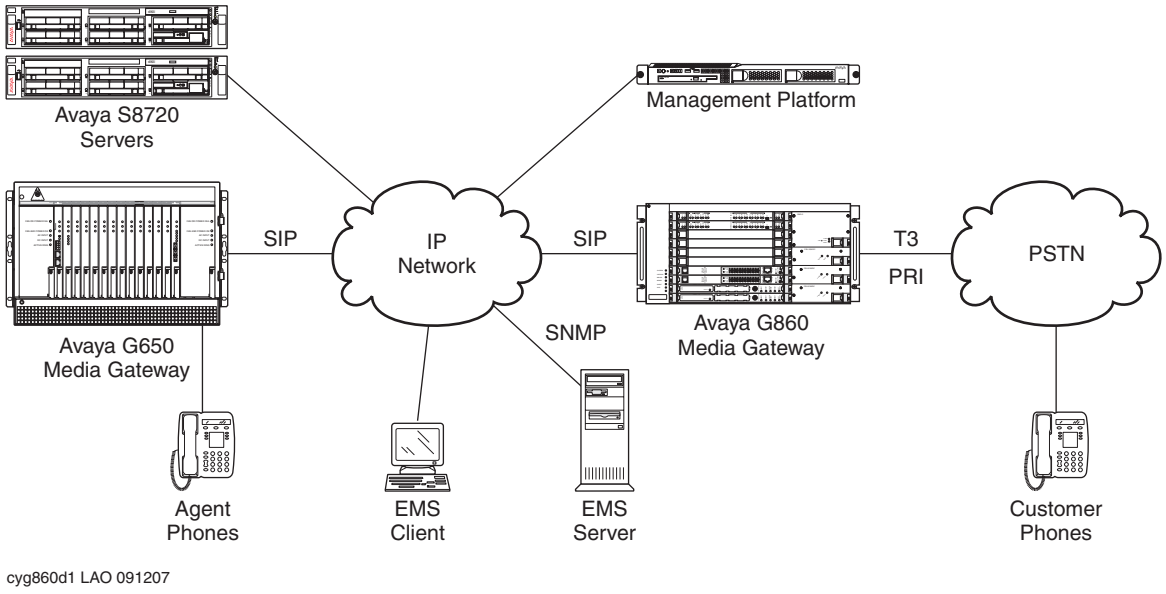
Example configuration for call center

The Avaya G860 Media Gateway allows call center customers to consolidate facilities and reduce communications costs. The media gateway concentrates incoming PSTN traffic over several DS3 lines while supporting VoIP telephony in the call center itself.

The use of voice over IP (VoIP) and conversion from DS1 to DS3 lines eliminate the large number of DS1 interfaces required to support the same amount of call traffic. The Avaya G860 Media Gateway supports up to 6000 channels of SIP VoIP telephony. It uses N+1 redundancy of media gateway, Ethernet switch, shelf controller, and power supply modules to achieve high availability in mission critical applications.

In the sample call center configuration shown in Figure 59, a simulated PSTN delivers customer calls using a DS3 interface to the Avaya G860 Media Gateway. The media gateway establishes calls with the Avaya S8720 or S8730 Server via SIP signaling and routes all Real-time Transport Protocol (RTP) traffic to the appropriate media resources within the Avaya G650 Media Gateway or Avaya endpoints. Avaya Communication Manager delivers the calls to an agent phone.

Figure 59: Sample call center configuration using the Avaya G860 Media Gateway



Agents can also make outbound calls using the same network. In the sample configuration, multiple TN799DP C-LAN circuit packs support alternate routing and permit load sharing of calls delivered by the Avaya G860 Media Gateway.

Note:

SES can be part of this configuration. The G860 communicates to Communication Manager over the LAN and SES is not needed between the G860 and Communication Manager for the G860 applications.

Mobility

IP Telephones or IP Softphones

IP Telephones allow access to the features of Communication Manager without having to be tied to one location. One of the major benefits of IP Telephones is that you can move the telephones around on an IP network just by unplugging them and plugging them in somewhere else. One of the main benefits of IP Softphones is that you can load them on a laptop computer, and connect them to the Communication Manager switch from almost anywhere. Users can place calls, and handle multiple calls on their PCs.

Extension to Cellular

Extension to Cellular is an integrated mobility solution that offers users the freedom to work anywhere, anytime, using any type of cellular or wireless telephone. With Extension to Cellular, calls to an office number are extended to a cellular telephone, allowing users to receive work-related calls wherever they are and whenever they need. Additionally, the cellular telephone can be administered so that when a user calls into the office, the user's name and office telephone number appear in the caller ID display of the telephone being called. When the Extension to Cellular cell phone is administered to send office caller ID, the user also has the option of picking up an ongoing Extension to Cellular cell phone call on the office telephone when the user enters the office.

Extension to Cellular works over PRI as well as an IP trunk interface. The cell phone user receives the same features and capabilities for incoming calls as a caller ID-enabled analog telephone that is connected directly to the Avaya Communications Server. Extension to Cellular provides this capability regardless of the cell phone's cellular service provider or the cellular standard in use.

Communication applications

Avaya Communication Manager supports a large number and variety of communication capabilities and applications, including:

- Call Center
- Messaging
- Unified Communication Center

- Avaya Call Management System (CMS)
- Conferencing systems
- Meet-me conferencing
- Avaya Meeting Exchange Solutions
- Video Telephony Solutions
- Computer Telephony Integration (CTI)
- Application Programming Interfaces (APIs)
- Best Services Routing (BSR) polling

For more information on these applications, see http://www.avaya.com/support.

Call Center

The Avaya Call Center provides a total solution for a customer's sales and service needs. Building on the performance and flexibility of the Avaya Communication Manager, customers can select from a powerful assortment of features, capabilities, and applications that are specially designed to enhance call center operations.

The objective of this offer, which involves new and existing versions of Avaya servers and Communication Manager, as well as a host of attached call center peripherals, is to improve Avaya's Call Center offers by supporting increased capacities. These capabilities include 6-digit and 7-digit extensions, LAN backup of Call Management System for the High Availability offer, and customer requested enhancements to be made available in a single global release.

Avaya Call Center applications are designed to efficiently connect each caller with the representative who is best suited to serve that caller. Avaya Communication Manager begins the process by capturing information about the caller even before the call is routed. That information is integrated with existing databases, and the combined data is used to match caller to agent.

Avaya Communication Manager integrates with a variety of Call Center applications like the Avaya Call Management System for real-time reporting and performance statistics, and with Avaya Business Advocate for expert predictive routing according to incoming calls, not just historical data.

Call Center applications

The Avaya Call Center solution is built on proven and innovative automatic call distribution (ACD) technology. This technology offers a suite of call routing capabilities that help agents handle calls more effectively. Customers can select from a powerful assortment of features, capabilities, and applications that are specially designed to enhance call center operations:

- Agent Access
- Avaya Call Management System

- Avaya Call Management System Supervisor
- Avaya Basic Call Management System
- Avaya Business Advocate
- Call Center
  - Avaya Call Center Basic
  - Avaya Call Center Deluxe
  - Avaya Call Center Elite
- Call Recording
- CALLMASTER® series digital telephones
- Computer Telephony (ASAI)
- Avaya Visual Vectors
- Avaya IP Agent
- Avaya Network Reporting
- Avaya Virtual Routing

Compact Call Center

The Compact Call Center application includes:

- Basic Call Management
- Reporting Desktop
- Computer Telephony

Messaging

The following messaging systems are supported by Avaya Communication Manager:

- INTUITY™ Messaging Systems
- Aria® Messaging Systems
- Serenade® Messaging Systems
- Modular Messaging®

Unified Communication Center

Unified Communication Center lets mobile, remote and office workers easily access important communications tools and information via any telephone using simple and intuitive speech commands.

Avaya Call Management System (CMS)

The Avaya Call Management System collects call traffic data, formats management reports, and provides an administration interface for Automatic Call Distribution (ACD) on your Communication Manager. CMS helps enterprises manage the people, traffic load, and equipment in an ACD environment by answering such questions as:

- How many calls are we handling?
- How many callers abandon their calls before talking with an agent?
- Are all agents handling a fair share of the calling load?
- Are our lines busy often enough to warrant adding additional ones?
- How has traffic changed in a given ACD hunt group over the past year?

Site Statistics for Remote Port Networks forwards location IDs to CMS to provide call center site-specific reports.

CMS reliability and redundancy

Dual Links to CMS provides an additional TCP/IP link to a separate CMS for full, duplicated CMS data collection functionality and high availability CMS configuration. The same data are sent to both servers, and the administration can be done from either server. The ACD data is delivered over different network routes to prevent any data loss from such conditions as ACD link failures, CMS hardware or software failures, CMS maintenance, or CMS upgrades.

Conferencing systems

Conferencing & Collaboration Applications enable cost effective means to connect with key people around the world in a way that enhances operations.

Meet-me conferencing

Meet-me conferencing provides conferencing of up to six parties from any communication device that is internal or external to the business network. This feature does not require any

special hardware. Meet-me conferencing uses a software approach that is based on Vector Directory Number (VDN) vectors and announcements. An announcement source is necessary to use meet-me conferencing. Supported announcement sources include:

- Voice Announcements over the LAN (VAL) circuit pack
- G700 local announcement
- Integrated Announcement circuit pack
- An external source

Avaya Meeting Exchange Solutions

Avaya Meeting Exchange is a family of comprehensive conferencing and collaboration solutions that extends proven Avaya conferencing features to support a variety of network protocols and enterprise implementations.

Meeting Exchange delivers proven voice quality and unsurpassed reliability in a solution that scales from ten to tens of thousands of users. Valuable features like Web Conferencing, conference scheduling and management tools, recording, reporting and customization capabilities are built in.

Meeting Exchange is interoperable with servers that run on open standards, and provides a variety of deployment options. Meeting Exchange supports pure Internet Protocol (IP), time division multiplexing (TDM) and mixed TDM/IP network environments. With Avaya Meeting Exchange, enterprises can migrate quickly and effectively to IP-based conferencing.

Meeting Exchange Enterprise Edition

Avaya Meeting Exchange delivers a host of features and capabilities designed to make conferencing easier, more flexible and more productive. These include:

Reservation-less Conferencing - Conferencing "on demand." Authorized conferencing users can arrange conferences on their own, whenever the need arises, without having to make arrangements ahead of time. Because the conference host has full conference control, order and security are well protected.

User Control of Conference Scheduling and Management - Maximize the value of the conferencing system by providing both users and operators access to easy-to-use scheduling and management tools, seamlessly integrated with enterprise conferencing platform.

Integration with Corporate Databases and Directories - Allows administrators to instantly establish or disable user accounts and maintain accurate user information.

Value-added Features - These capabilities, including reporting, recording and billing, enable enterprises to precisely manage use of their conferencing service by generating customized conference reports and enabling internal bill back systems.

Integrated Web Conferencing - Provides comprehensive collaboration capability including distribution of graphics and presentations, application viewing and sharing, white boarding, and optional conference recording and playback.

Easy Scheduling - Integrated Microsoft Outlook or Lotus Notes calendar and web capabilities make it simple to schedule conferences and notify participants using these familiar desktop productivity tools.

Open Architecture - Enables seamless integration with a range of applications and services. API-based developer tool kits allow development of integrated or custom features and applications.

Integration Options - Avaya Meeting Exchange offers integration with corporate directories and databases using standard Lightweight Directory Access Protocol (LDAP), for simple maintenance of corporate accounts. Multi language options provide for translated conference prompts and greetings. A Multi Site option reduces networking costs and network traffic by linking multiple conference systems in dispersed locations.

Table 20: Meeting Exchange Conferencing Servers Feature and Capacity

	CS700	CS780	C6200	S6800	S6100
Protocols	TDM	TDM	TDM, IP or Mixed	IP	TDM, IP or Mixed
Capacity	T1: 1152 ports E1: 1200 ports T3: 2016 ports ISDN: 1104 ports	T1: 576 ports E1: 600 ports ISDN: 552 ports	IP: 240 ports T1: 192 ports E1: 240 ports ISDN: 184 ports	9,000 ports (per chassis)	300 ports
					1 of 2

Table 20: Meeting Exchange Conferencing Servers Feature and Capacity (continued)

	CS700	CS780	C6200	S6800	S6100
Features	Carrier-grade, high survivability and reliability. Available as AC or DC. Variety of redundancy options (RAID 5, N+1 P/S) Hot swappable components.	Carrier-grade, high survivability and reliability. Available as AC or DC. Variety of redundancy options (RAID 5, N+1 P/S) Hot swappable components.	Based on an IBM x336 1U server. Includes redundant hard disks and power supplies.	Based on Convedia CMS-6000 Media Server. S6200 is used as an Application Server. Available as AC or DC. Variety of redundancy options available.	Based on an IBM x336 1U server. Includes redundant hard disks and power supplies.
Networks	T1, E1, T3, or ISDN from PBX or telecom provider	T1, E1, T3, or ISDN from PBX or telecom provider	IP Trunks, T1, E1, or ISDN from PBX or telecom provider	IP Trunks from PBX or telecom provider	IP Trunks, T1, E1, or ISDN from PBX or telecom provider
					2 of 2

Meeting Exchange Web Conferencing

Target Market: Mid-market, Service Providers

Integrated Solution Features:

- PowerPoint push and document annotation, white boarding, chat, polling
- Desktop or application sharing
- Workhorse application for 4-8 person, everyday meetings
- Customizable
- Integration w/ Meeting Exchange audio conferencing: synchronized recording and playback of audio and web portions of the conference, Integrated participant roster (control audio and web participants)

Strengths and Differentiators - Meeting Exchange Web Conferencing offers intuitive application with features most-used by Web conferencing users. It is scalable, secure behind-the firewall solution. The application is ideal for a 4 to 8 person meeting. It provided optimized bandwidth for users with any connection speed.

Hardware and Software requirements include:

- Meeting Exchange audio conferencing bridge
- Off-the-shelf server, plus Web Conferencing software (license based capacity)
- Additional servers required for recording and playback (optional)

Meeting Exchange Express Edition

Meeting Exchange Express Edition Release 1.5 is an audio conferencing server aimed at mid-market enterprise customers. It offers a Voice over Internet Protocol (VoIP) or Time Division Multiplexing (TDM) solution for up to 300 concurrent users. It supports scheduled and reservation-less conferencing through a Web interface where conference hosts can create, edit, and delete conference reservations for single instance and recurring bookings.

Meeting Exchange Express Edition ships with an optional plug-in for Microsoft Outlook. This plug-in enables users to schedule conferences using the Microsoft Outlook application. A Conference Call tab displays in the existing New Appointment screen and enables conference hosts to book scheduled conferences or retrieve their on-demand conference details, using the standard Microsoft Outlook calendar and invitation functions.

Meeting Exchange Express Edition is fully compatible with the Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory 2003. It is also fully integrated with Communications Process Manager 2.0 (CPM). CPM users can create exception conferences in the CPM interface which are managed by Meeting Exchange Express Edition as ad hoc conferences. In addition, Meeting Exchange Express Edition can inform CPM of active conferences on the server using a SIPPING subscribe/notify mechanism.

Meeting Exchange Express Edition can be integrated with IBM Sametime 7.5 application, using the IBM Lotus adaptor 1.0.5. This integrated solution allows users to Click-to-Conference from the Sametime Connect client. It also provides embedded audio conference controls in the Sametime Web Meeting, enabling conference hosts to identify speakers, mute one or many participants, and dial out to bring new people into the call, among other capabilities.

Meeting Exchange Express Edition Release 1.5 is localized into a number of languages, including German, Korean, Japanese, and Simplified Chinese. Avaya has translated the GUI interfaces, the documentation suite, and all audio message recordings.

For more information, see *Meeting Exchange Express Edition Release 1.5 Installation and Configuration Guide* (04-601898), *Meeting Exchange Express Edition Release 1.5 Administration and Maintenance Guide* (04-601909), *Meeting Exchange Express Edition Release 1.5 User Guide* (04-601910), and *Meeting Exchange Express Edition Release 1.5 Release Notes* (04-601913).

Video Telephony Solutions

The Avaya Video Telephony Solution enables Avaya Communication Manager to merge a set of enterprise features with Polycom's video conferencing adjuncts. It unifies voice over IP with video, web applications, Avaya's video-enabled IP Softphone, third-party gatekeepers, and

other H.323 endpoints. With the Avaya Video Telephony Solution, you can provide video for desktop and group communications.

The Avaya Video Telephony Solution supports the following features and products:

- Ad-hoc video conferencing
- Avaya IP Softphone Release 5.2 or 6.0 and Video Integrator
- Polycom VSX-series video conferencing systems
- Ploycom RMX 2000 and MGC video conferencing bridge platforms
- Ploycom HDX video conferencing system
- Polycom V500 video calling system
- Third-party gatekeepers, including the Polycom Path Navigator gatekeeper
- 3G gateways
- H.320 gateways

Computer Telephony Integration (CTI)

Computer Telephony Integration (CTI) enables Communication Manager to be controlled by external applications, and allows integration of customer databases of information with call control features. CTI is a LAN-based solution that consists of server software that runs in a client/server configuration.

CTI opens up Application Programmer Interfaces like ASAI, Telephony Services Application Programming Interface (TSAPI), and Java Telephony Application Programming Interface (JTAPI), which can be used to control the server from an external application.

Application Programming Interfaces (APIs)

Communication Manager supports the following APIs to interface with other applications:

- Adjunct Switch Application Interface (ASAI) allows adjunct applications to access a collection of Communication Manager features and services. Integration with adjuncts occurs through APIs. ASAI is part of Avaya Computer Telephony.
- DEFINITY Application Programming Interface (DAPI) for accessing control and data paths within Communication Manager.
- Java Telephony Application Programming Interface (JTAPI) is an open API supported by Avaya Computer Telephony that enables integration to Communication Manager ASAI.
- Telephony Application Programming Interface (TAPI).
- Telephony Services Application Programming Interface (TSAPI) is an open API supported by Avaya Computer Telephony that allows integration to Communication Manager ASAI.

Best Services Routing (BSR) polling

Best Service Routing (BSR) polling over QSIG Call Independent Signaling Connections (CISCs) and Temporary Signaling Connections (TSCs) provides the ability to do BSR polling between multiple sites over H.323 IP trunks without requiring an ISDN PRI B-channel. QSIG CISC/TSCs are used by BSR polling software to reduce the need for the IP Media Processor circuit pack, thereby making BSR a cost-effective, multi-site solution for an enterprise-wide contact center.

LAN switching products

This chapter discusses how Avaya LAN switches and other LAN switching products add value to an IP Telephony deployment.

Avaya C360 converged stackable switches

The Avaya C360 converged stackable switch series is a line of stackable, multilayer switches that provide high availability, quality of service (QoS), and Power over Ethernet (PoE) to enhance converged network infrastructure operations. With a range of PoE and non-PoE configurations, the C360 series is a powerful, yet cost-effective option for enterprise applications. The C360 series offers a migration path for the P330 series, and can be stacked with P330 switches and G700 Media Gateways.

The Avaya C360 series of converged stackable switches includes:

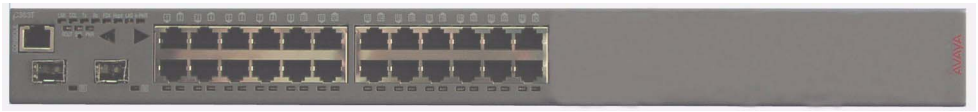
- A range of modules with 24 or 48 10/100 Mbps ports supporting PoE or non PoE and two GBIC SFP slots for Gigabit Ethernet connections
- A Layer 3 capability

The available C360 switch models are as follows:

- C363T converged stackable switch

  This switch has 24 10/100 Mbps ports and two GBIC SFP ports.

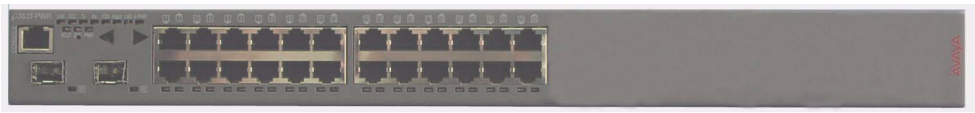
Figure 60: C363T Converged Stackable switch



- C363T-PWR converged stackable switch

  This switch has 24 10/100 Mbps ports with Power over Ethernet (PoE) and two GBIC SFP ports.

Figure 61: C363T-PWR Converged Stackable switch



- C364T converged stackable switch

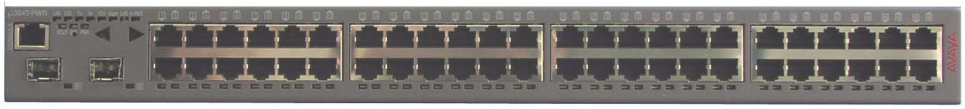
  This switch has 48 10/100 Mbps ports and two GBIC SFP ports.

Figure 62: C364T Converged Stackable switch

- C364T-PWR converged stackable switch

  This switch has 48 10/100 Mbps ports with Power over Ethernet (PoE) and two GBIC SFP ports.

Figure 63: C364T-PWR Converged Stackable switch



A C360 switch can co-reside in a stack with G700 media gateways and with selected P330 switches. A C360 stack can contain up to 10 switches and up to three backup power supply units. The stacked switches connect using the stacking sub-modules that plug into a slot in the back of the C360. The X330RC cable connects the top and bottom switches in the stack and provides redundancy and hot-swappability in the same way that modules can be swapped in a modular switching chassis.

Avaya C360 switches are multilayer switches and can be upgraded with a license to provide routing (Layer3) functionality.

Features of the C360 converged stackable switches

The C360 Converged Stackable switches offer features in the following categories:

Stacking

- Up to 10 switches can be stacked together.
- Features such as Spanning Tree, redundancy, VLANs, and SMON are common to the stack.
- The Octaplane stacking system provides 8 Gbps stacking bandwidth to all switches in the stack.
- C360 stacks continue to function even if one switch or link fails.
- Switches in the stack can be added, removed, and replaced without disrupting operation.
- An advanced election algorithm ensures optimal stack master selection.

Layer 2 features

- Auto-sensing simplifies configuration of LAN connections by automatically selecting the port speed for devices — either 10Mb or 100Mb.
- Auto-negotiation simplifies configuration of LAN connections by automatically selecting the port transmission mode for devices — either half- or full-duplex.
- Auto-MDIX automatically adjusts for straight-through or crossover cables on all 10/100-TX ports.
- Traffic prioritization (802.1p) allows real-time traffic classification into 8 priority levels mapped to 4 queues.
- There are four egress queues on all switch ports. The queues can be configured with the WRR (Weighted Round Robin) or strict priority scheduling algorithm.
- The use of the IEEE 802.1Q tagging for VLANs and per-port VLAN is supported.
- Multiple VLANs per port allow access to shared resources by stations that belong to different VLANs.
- The use of the IEEE 802.1w standard for Rapid Spanning Tree Protocol (RSTP) provides rapid convergence of the spanning tree in case of link failure.
- The use of the IEEE 802.1x standard for port-based network security ensures that only authorized clients get network access.
- Up to 20 redundant-port pairs are supported to increase link resiliency.
- Inter-module redundancy is supported with one pair in a stack. The switching time is approximately 1 second.
- Link Aggregation Group (LAG) support of up to 7 trunks, with each trunk having up to 8 10/100 links or 2 GB links, provides resiliency, load balancing, and bandwidth expansion.
- LAG redundancy is supported through resiliency between two LAG groups.
- Port mirroring of any switch port is supported.

- RMON/SMON port statistics provide real-time top-down analysis of network traffic.
- IP multicast filtering (snooping) filters multicast traffic to optimize network bandwidth.
- Classification of ports as regular or valuable is supported so that if a link fails, notification is generated for valuable ports only.
- The L2 CAM table contains 16K MAC addresses.

Layer 3 features

Note:

An additional license is required for Layer 3 features.

- Static, RIPv1, RIPv2, OSPF IP routing protocols are supported.
- Equal cost routing is used for load balancing and redundancy.
- Router redundancy (VRRP) is supported.
- NetBIOS rebroadcasting is available for applications such as WINS that use broadcasting but may need to also communicate with stations on other subnets or VLANs.
- ICMP and ARP protocols are supported.
- DHCP/BootP relay allows broadcast requests to be forwarded to servers.
- Policy-based routing of packets provides enforcement of QoS and ACL rules.
- The L3 CAM table contains 4K IP addresses.

Management

- Access to the management interfaces are password-protected at three levels (read-only, read-write access and supervisor) to prevent unauthorized configuration changes.
- You can access to the Command Line Interface (CLI) in the following ways:
  - Direct console or modem connection
  - Telnet (up to five simultaneous connections) or SSHv2 (up to two simultaneous connections) over the IP network
- You can use TFTP for the download/upload of configuration files or the download of firmware files
- You can use SCP (Secure Copy Protocol) for secure download/upload of configuration files
- You can use SSH encrypted login sessions as a secure way to manage the switches remotely.
- A Java-based Device Manager provides an intuitive Web-based interface for access
- SNMPv1 is supported.

- Simple network time protocol (SNTP) or TIME protocols are available to provide a consistent timestamp to all switches from an external source.
- Radius authentication enables centralized user management.
- You can use all appropriate tools of the Avaya Integrated Management suite for administration.
- System logging can occur by terminal, internal file, or Syslog server.
- Switch access can be restricted to specified protocols or services.
- You an restrict access to management interfaces by IP address.
- You can invoke a telnet client from the CLI.

Power over Ethernet (PoE)

- PoE is supported on the C363T-PWR and C364T-PWR switches.
- PoE is fully compliant with the 802.3af-2003 standard.
- PoE provides up to 15.4W per port (on10/100 ports) over Ethernet cables to power IP phones, wireless access points, and other end-points using 802.3af-2003 standards.
- PoE automatically detects device connections and removal.
- PoE automatic load detection does the following:
  - Tests whether the device connected to the port requires remote powering.
  - Controls the power injection to the wires.
- Power is distributed between the 24/48 PoE ports according to priorities that you configure. Power priority can be configured on each port. Distribution is calculated from actual power consumption.

Switches from Extreme Networks

Avaya recommends the following switches from Extreme Networks for use with Avaya VoIP:

- Fixed switches (access layer)
  - Summit X250e-24p - a 24-port stackable switch that provides PoE.
  - Summit X250e-48p - a 48-port stackable switch that provides PoE.
  - Summit X450e-24p - a 24-port non-blocking 10/100/1000 stackable switch that provides PoE
  - Summit X450e-48p - a 48-port non-blocking 10/100/1000 stackable switch that provides PoE
- Chassis-based switches (access, distribution and/or core layers)

- BlackDiamond 8806 - a 6-slot non-blocking switch for access or core
- BlackDiamond 8810 - a 10-slot non-blocking switch for access or core

For information on Extreme Networks switches, see http://www.extremenetworks.com

Avaya Power over Ethernet (PoE) switches

For more information on Power over Ethernet (PoE), see A Practical Guide to Power over Ethernet by Avaya, using the following link: PoE Guide

Available PoE Switch Options

Data and power are combined in a (PoE) switch and sent over a single cable, thus simplifying power management and cabling infrastructure and saving rack space.

Avaya offers the following PoE Converged Stackable Switches: C363T-PWR and C364T-PWR.

All PoE Switches comply with the IEEE 802.3af standard.

Switch	Maximum PoE Power (W)	Number of Powered Ports in Switch
C363T-PWR	305	24
C364T-PWR	520	48

PoE is carried over the signal leads, providing remote -48V power feeds on all 10/100 ports in the switch/module (except on an expansion module in P333T-PWR). This allows the PD (Powered Device) to be up to 100m away from the switch. Each port performs a standard compatibility detection process before power is supplied to the Ethernet lines. If the PD is removed or the link is interrupted, the port polling mechanism detects this, and power is cut off to the port while the detection process is applied again.

The PoE switch applies power to the port only after it detects that a PD is actually connected to the port. Each PD has a resistance range known as a "signature." The switch knows what power has to be supplied to the device according to the signature.

Load detection is performed every 240 ms. All ports are checked for the resistance signature on a port-by-port basis. Only non-powered ports participate in the periodic load detection. Once power is provided to a port, it is checked periodically to see if a PD is still connected. If a PD is disconnected from a powered port, then power is denied to the port. Disconnected ports then automatically join the periodic load detection cycle. Each port of the switch is protected against channel overload, short circuit, and reversed polarity that might be caused by faulty connection between two feeding channels or by a crossed cable connection.

Power priority mechanism

The priority mechanism is implemented in order to handle cases where the power requested by the PDs exceeds the switch PoE capacity. This priority mechanism determines the order in which ports will be powered on after boot, and powered off if the power resources of the module are exhausted. Three user-configurable port power priority levels are available: low, high & critical. Within each priority level the lower the port number, the higher the priority (by default all the ports have low priority).

Disconnected power will be automatically reconnected to the PDs based on their priority, whenever there is an available power budget. Immediately after the PoE has booted up, it starts to supply power to the ports where a load is detected. Ports are powered up one after another, based on the port priority, until the limit is reached. Power calculation is based on the actual power consumption of the PD. After this, no more ports are powered up until the total power consumption drops lower than the limit. The limit is 18 Watts below the maximum PoE capacity. The remaining 18W are reserve power for a change in the power draw of PDs.

Midspan Power Units

1152A1 Power Distribution Unit

The official name for this device is the 1152A1 Power Distribution Unit, but the Midspan Power Unit can also be called a powered data unit (PDU) or a power over Ethernet (POE) device. The Midspan Power Unit is 1U in height (1.75 inches or 4.44 cm) and has 24 RJ45 data input jacks on the bottom row, and 24 data and power output RJ45 jacks. Data flow is unaffected if power is disrupted and if the endpoint does not require power. An example is a laptop computer that is connected to the 1152A1. The computer does not receive power from the 1152A1. If the 120-volt power is disrupted to the 1152A1, the computer data stream would not be affected. The 1152A1 unit provides a maximum of 200 watts or a peak of 16.8 watts per port. This unit powers any device that conforms to the 25-K Ohm resistive signature defined in the IEEE 802.3-2003 af standard. This unit also powers devices that use the nonstandard capacitive signature, such as Cisco IP telephones. The 1152A1 provides positive voltage on pins 4/5 and negative voltage on pins 7/8, which is one of the three methods as described by the IEEE 802.3af standard.

Designed usage

The Midspan Power Unit is designed to mount in a 19-inch data rack, or can be stacked up to four units high using the optional rubber feet. Its niche is to provide power to only those IP endpoints that need power. The alternative is to have a switch that incorporates power. However, any nonpowered device that uses that switch is not using the power capabilities of the switch, and does not justify the higher price per port of that switch. The Midspan Power Unit solves this problem by providing power without altering the network topology.

The 1152A1 can be collocated with the data equipment or closer to the endpoints. In all cases, IEEE 802.3af capable IP devices must connect directly to this PDU. The PDU cannot power any device if a hub or a switch is between itself and the endpoint because it will not sense the resistive signature needed to authorize the release of power.

Power modes (Avaya IP Telephones)

The Avaya IP Telephone has four different power modes:

- Ethernet spare pairs (4/5 and 7/8)
- Ethernet signaling pairs (1/2 and 3/6)
- Traditional telephony (7/8)
- (4630 model only) External transformer with a barrel connector

The 1152A1 power unit powers only through pairs 4/5 (+) and 7/8 (-).

Barrel connector through brick transformer

This brick type transformer provides 5 watts of power to the telephone. The Avaya telephone treats this brick as the primary power source, and will *not* accept power from the Ethernet cable if the barrel is seated into the telephone, with or without the brick attached to AC power.

Ethernet cable through 1152A1 PDU

Adequate power from the 1152A1 is supplied to the generation 2 telephones over the Ethernet cable. Category 5 or better cable is required for Fast Ethernet to function from the IP Telephone.

Power using adapters

Generation 1 telephones can receive power from the 1152A1 through an in-line adapter. This adapter provides the resistive signature so that the 1152A1 allows power to flow to the telephone. The generation-2 telephone does not need an adapter, but it might mistakenly be used on a generation-2 telephone. Both generation phones work as designed through all tests performed in Avaya labs.

Interoperability with Wireless Access Point products

The 1152A1 unit can also power Avaya's Wireless Access Point systems. The AP1, AP2, or AP3 act as a bridge between the wireless and the wired LAN. This system requires a 5-volt power supply that can be replaced by a splitter, which fits in the same cavity as the original power converter and allows power over the Ethernet, eliminating the need to find a power source close to the unit.

1152B Power Distribution Units

The Avaya 1152B Mid-Span Power Distribution Units are Ethernet power supplies that provide power to up to 48 46xx-series or 96xx IP telephones or wireless LAN (WLAN) access points. The 1152B PDUs are designed to deliver power in addition to data communication over an Ethernet network. The 1152B PDUs eliminate the need to connect each Ethernet Data Terminal, such as an IP Telephone set, to an AC power outlet in addition to the data port. The system also removes the need for power cables, local AC wall adapters and the use of a dedicated UPS for each IP telephone. Some models support SNMP remote management via a separate physical RJ45 input port.

These units are used with a standard 10/100BaseTx Ethernet network infrastructure using standard TIA/EIA-568 Category 5, 5e, or 6 100-Ohm Unshielded Twisted Pair (UTP) cable. The 1152B meets the current requirements of the IEEE802.3af-2003 standard for resistive detection.

The units are as follows:

Table 21: 1152B Midspan Power Distribution Units

Avaya Model Number	Number of Ports	SNMP	Summary
1152B48S	48	Yes	48-port, AC Input, 48Vdc Output with SNMP
1152B24S	24	Yes	24-port, AC Input, 48Vdc Output with SNMP
1152B06	6	No	6-port, AC Input, 48Vdc Output
1152B06S	6	No	6-port, AC Input, 48Vdc Output with SNMP

The 1152B PDU complies with the Underwriters Laboratories Inc. (UL) standard UL 60950-1, 1st Edition.

Table 22: 1152B PDU UL 1950 Compliance

Complies	UL 1950
Approved	CAN/CSA-C22.2 No. 60950-1-03Std.
Approved	CE Regulatory Compliance
Approved	EN 60950
Approved	TUV EN 60950

Designed usage

The 1152B PDUs are used to power the 46xx series and 96xx series of IP telephones in addition to providing 10/100 megabits per second Ethernet connection.

Generation 1 Avaya IP telephones can receive power from the 1152B using an in-line adapter. This adapter provides the resistive signature so that the 1152B allows power to flow to the telephone. The generation 2 telephones do not need an adapter.

The 1152B PDU has 10/100 Base-T ports, each of which can supply a minimum of 15.4 watts using the internal power supply and operates on a 100-240 volts AC, 60/50 hertz power source.

The 1152B PDU is 1U high and fits in most standard 19-inch racks. It can also be mounted on a shelf. Refer to the user's guide that comes with the unit for complete installation instructions.

Converged infrastructure security gateways

For information on the Avaya security gateways, please visit the following web sites.

SG200

The SG200 Security Gateway is a VPN/firewall device designed for branch office and small/mid-sized enterprise deployments.

http://www.avaya.com/gcm/master-usa/en-us/products/offers/sg200.htm

SG203 and SG208

The SG203 and SG208 Security Gateways integrate advanced stateful firewall, VPN, bandwidth management, and IP telephony management capabilities for distributed mid-to-large enterprises with IP contact centers or converged voice/data networks.

http://www.avaya.com/gcm/master-usa/en-us/products/offers/sg203_sg208_security_gateways.htm

VPN Client

VPNremote® Client offers cost-effective, easy-to-install remote VPN connectivity that helps increase the productivity of telecommuters and mobile workers by providing secure, simple-to-use access to your enterprise network from any Internet access point.

VPNremote Client is a compatible with Microsoft Windows software, and provides secure, authenticated access to enterprise network resources and applications over the Internet. This application leverages the benefits of global access and cost-effective public network features to support a remote or a mobile work force. VPNremote Client not only provides support for data applications, but also delivers voice-over-VPN that enables you to use the Avaya IP Softphone for secure, convenient telephony from your laptop computer. To protect the integrity and confidentiality of data that travels outside of an enterprise network, VPNremote Client uses standards-based IPSec technology to provide strong two-factor authentication, robust 3DES encryption, and data compression.

VPNremote Client overcomes the complexities that are typical of deploying a remote access solution. Easy installation and dynamic configuration dramatically reduces the burden for both end users and administrators. The intuitive graphical user interface-based Connection Manager helps you easily log on to your VPN by selecting a preconfigured user profile and entering your password. User profiles can also be exported to enable users to connect to the VPN from any computer using VPNremote. VPNremote also supports mobility by allowing users to securely connect to many wireless LAN systems.

Section 2: Deploying IP Telephony

Traffic engineering

This chapter provides an introduction to traffic engineering. Specifically, this chapter discusses various traffic models, algorithms, and resource sizing.

This section includes the following topics:

Introduction

The process of configuring, engineering, and deploying a Communication Manager system, or a network of Communication Manager systems, begins with specifying the quantity and the nature of the endpoints to be accommodated. Principles of traffic engineering are then applied to determine the quantity and the placement of the various necessary resources. Once the designed configuration adheres to all specifications and system constraints, the process is finished.

This discussion of the configuration, engineering, and deployment processes is intended as an overview that is suitable for a fairly general audience. One example that is designed to exercise all aspects of these processes continues throughout the chapter to present the finer points of network design.

Design inputs

This section summarizes the essential design elements that the customer must specify.

Topology

An Avaya Communication Manager system consists of a server and all of the equipment under that server's control. Such equipment may be geographically dispersed among a variety of sites, and the equipment at each site may be segregated into distinct logical collections known as Network Regions. In cases where one server is insufficient for controlling all of the equipment, multiple Avaya systems can be networked together. So, a *Network Region* is a component of a *site*, which is a component of a *system*, which is a component of a *network*.

A single Avaya Communication Manager system is comprised of one or more *Network Regions*. Each Network Region is a logical grouping of endpoints, including stations, trunks, and Media Gateways. Customers can choose to establish various Network Regions on the basis of geography, business sectors, or any of a variety of other considerations. For example, a customer with facilities in both New York and Los Angeles might choose to use a single Communication Manager system, with one Network Region in each of the two cities. Another possibility is to assign two Network Regions to each city. In that case, each such geographical grouping of Network Regions is said to comprise a *site*.

Alternatively, that same customer might want to administer three Network Regions, where one region corresponds with Sales and Marketing, another with Customer Support and Services, and a third with Research and Development. In this case, the Network Regions are established independently of geographical considerations, because associates from each of the three distinct business sectors may be physically located in both cities. Yet another possibility is to construct Network Regions to correspond with IP subnets.

The various Network Regions within a Communication Manager system are interconnected by an IP network. An IP network can consist of local area networks (LANs), wide area networks (WANs), or a combination of both LANs and WANs. A common approach is to use a LAN at each site, and interconnect those LANs through a WAN. Because Network Regions are used to specify differences between the treatment of intrasite and intersite traffic, or to properly select localized media resources for optimal voice quality, Network Regions should not span multiple geographical locations.

A Communication Manager system can operate as an independent entity, or can be networked together with other Communication Manager systems. For networked systems, the various Communication Manager systems in the network are generally interconnected by IP tie trunks. If the two members of a given pair of Communication Manager systems in a network are not directly interconnected by tie trunks, calls between the two systems must be tandemed through other Communication Manager systems in the network.

When there is a need to accommodate endpoints in various geographic locations, the customer has the choice to either set up a single Communication Manager system with a site at each location, or use a network of multiple Communication Manager systems to span the locations. The choice of which one is more appropriate pertains to the issue of scalability. An extremely large number of endpoints might mandate the use of multiple systems.

While Communication Manager systems have been designed with an IP infrastructure, they also support circuit-switched endpoints, and the full complement of traditional DEFINITY features. However, customers usually realize a significant advantage when those customers implement an IP-oriented solution for systems that are geographically dispersed.

Each endpoint and Media Gateway is assigned to a Network Region when its IP address is administered. Also, each Network Region is administered with a codec preference list, which is a list of up to five codecs that are supported by that Network Region. Uncompressed G.711 and compressed G.729 are the most commonly used codecs in Communication Manager systems. Each Communication Manager system is administered with the Internetwork Region Connection Management (IRCM) matrix, which provides enough information to specify which codecs to use when completing a call between Network Regions.

Conversely, if the IRCM does not specify a codec set between two Network Regions, calls cannot be completed between those regions over an IP connection. For instance, the manager of an office building can use a single Communication Manager system to service all the individual lessees, with a separate Network Region for each company. Those Network Regions generally would not be connected by the IRCM because independent companies would be unwilling to share each others' resources. Subsequent sections of this chapter further explain sharing resources across connected Network Regions.

Multiple Communication Manager systems are often networked together by IP tie trunks, although circuit-switched tie trunks can also be used. If the two members of a given pair of Communication Manager systems in a network are not directly interconnected by tie trunks, calls between the two systems must be routed through other Communication Manager systems in the network, or through the public switched telephone network (PSTN).

Although Avaya products are IP enabled, the products must interface with circuit-switched endpoints and systems. For example, Communication Manager systems require circuit-switched trunks to access the PSTN because central offices today are not equipped for IP trunking. Some customers also prefer to continue to use their circuit-switched telephones in Communication Manager systems.

Circuit-switched endpoints interface to circuit packs that reside in media gateways or traditional port networks (PN). Although each media gateway belongs to one particular Network Region, no correlation exists between PNs and Network Regions. PNs are interconnected through a circuit-switched center stage or an ATM center stage (S8700 fiber-PNC systems) or an IP network (IP-PNC systems).

Endpoint specifications

Normally, a customer who submits a Request for Proposal (RFP) specifies the number of each type of station to place in each site, in each Communication Manager system in the network. Certain customers might want to specify station placement more precisely. For example, a customer might specify the exact population of circuit-switched stations on a Media Gateway.

The majority of customers know exactly how many of each station type are needed at each site, based on the population of their anticipated end-users. However, the issue of trunk sizing is not as straightforward. Trunk traffic is tightly coupled with station traffic because at least one party in every Communication Manager trunk call is a Communication Manager station (except in relatively rare cases in which a Communication Manager system is used to tandem calls between non-Communication Manager endpoints). That being the case, station traffic effectively induces trunk traffic. The given topology of trunk groups dictates which pairs of Communication Manager systems are directly connected by trunks, and which Communication Manager systems are directly connected to the PSTN (or other non-Communication Manager systems). However, the size of each trunk group must be engineered with consideration of the amount of traffic that each such trunk group is anticipated to carry. A traffic engineer should either specify the number of trunks in each trunk group directly, or allow the configuration algorithm to size the trunk groups to a specified Grade of Service (GOS). This GOS is usually P01, which is 1% blocking. In some cases, customers might choose to over-engineer or under-engineer certain trunk groups based on non-traffic considerations, such as reliability, cost, security, and so on.

Endpoint traffic usage

Traffic usage is typically expressed in Erlangs, which represent the average number of busy servers in a given server group. For example, if a group of stations carries 100 Erlangs of call usage, that means the average number of those stations that are busy at any given time is 100. The usage of a single station, when expressed in Erlangs, represents the fraction of time that the station is in use. So, a station that carries 0.1 Erlang of usage is in use 10% of the time.

The most common way to specify total station usage is to multiply the usage per station by the total number of stations. A traffic engineer can either explicitly specify the per-station usage for each group of stations, or allow the configuration algorithm to specify per-station usages automatically, using default values. Common defaults for station traffic usage in general business scenarios are:

- **Light** traffic—0.056 Erlangs per station (stations average 5.6% usage)
- **Moderate** traffic—0.11 Erlangs per station (stations average 11% usage)
- **Heavy** traffic—0.17 Erlangs per station (stations average 17% usage)

The most commonly used default value for a general business system is 0.11 Erlangs per station. The most common way to determine trunk usage rates is to divide the total traffic load that is carried by each trunk group by the number of trunks in the group. It is difficult to assign a typical default value for usage per trunk. Such usage can vary greatly from system to system, and even from trunk group to trunk group within a particular system.

Traffic usage has two components:

- Average call duration (also known as call *hold time*)
- Average number of calls per hour

Systems are usually engineered to accommodate the busiest hour of a normal business day. The number of calls that are completed during that busiest hour is denoted by Busy Hour Calls Completed (BHCC). BHCC is not be confused with Busy Hour Calls Attempted (BHCA), which represents the total number of calls attempted during the busiest hour, regardless of how many of those calls are actually successfully completed. The general expression for the relationship between BHCC, average call duration, and usage is:

$$\text{Usage (Erlangs)} = \frac{\text{BHCC} \times \text{seconds per call}}{3600}$$

A commonly used default value for average call duration in a general business system is 200 seconds per call. Example 1: Station usage shows how to calculate the station usages using the data given.

Example 1: Station usage

Assume that an enterprise has sites in Atlanta, Boston, and Cleveland that it wants to populate with the following endpoints (Table 23: Example 1 configuration data on page 181).

Table 23: Example 1 configuration data

Endpoints	Atlanta	Boston	Cleveland
DCP Telephones	540	180	
IP Telephones	1,080	450	270
Analog stations	108	18	
Road Warriors	27		
Other			Two G350 Media Gateways, each of which supports 18 analog stations, and a suitable number of circuit-switched PSTN trunks

Additional design criteria

- Each site is to have a suitable number of PSTN trunks (which terminate on PNs in Atlanta and Boston, and on the G350 Media Gateways in Cleveland).
- This is a general business application (for example, no Call Center agents), where the average usage per station is assumed to be 0.11 Erlangs, and the average call duration is assumed to be 200 seconds.
- Each site consists of a single Network Region, and all three Network Regions are interconnected in the sense of the IRCM matrix.
- One-third of all calls are intercom calls (that is, calls between two stations), one-third are inbound PSTN trunk calls, and one-third are outbound PSTN trunk calls.

Preliminary calculations

Based on the assumption of 0.11 Erlangs per station, Table 24: Example 1 station usage by endpoint type on page 182 shows the total station usage for each station category in the system.

Table 24: Example 1 station usage by endpoint type

Endpoints	Atlanta (Erlangs)	Boston (Erlangs)	Cleveland (Erlangs)
DCP Telephones	60	20	
IP Telephones	120	50	30
Analog stations	12	2	
Road Warriors	3		
Analog stations administered to G350 Media Gateways			4

Call usage rates

In the previous section, station usages and overall endpoint usages, including both stations and trunks, were discussed. The overall endpoint usage is sometimes referred to as port usage rate (PUR). The term station usage rate (SUR) applies when referring only to the stations. In general, a traffic usage rate, when expressed in Erlangs, represents the average number of busy servers in a given server group. So, SUR represents the average number of stations in a particular group that are simultaneously in use, while PUR represents the average number of endpoints, including stations and trunks, in a particular group that are simultaneously in use.

Similarly, the term call usage rate (CUR) represents the average number of simultaneous calls that are carried by a particular facility. In an environment where essentially every call is either inbound or outbound (such as a call center), CUR and SUR are equal, because there is exactly one Communication Manager station used in each call. However, in an environment such as a general business scenario in which some calls are intercom, some calls are inbound, and some calls are outbound (such as a General Business scenario), CUR and SUR are not equal, because some calls (the intercom calls) use two Communication Manager stations, and others (inbound and outbound calls) use only one Communication Manager station.

The next step in the configuration process is to determine the amount of traffic flow between Communication Manager systems in a network, and between the sites in each individual Communication Manager system. Those traffic flows can be further refined to identify the traffic flows between the various categories of endpoints within each site. All such traffic flows can be represented in tabular form.

Communities of interest

The various sites within a particular Communication Manager system comprise *communities of interest* (COI), in the sense that the endpoints in each particular site share some common trait or interest, usually geographical proximity. A COI matrix offers a convenient representation of the traffic flows between the various sites. For example, consider the COI matrix in Table 25: 3-site standalone community of interest (COI) matrix on page 184 for a three-site, stand-alone Communication Manager system.

In practice, a COI matrix that is associated with a given system is populated with actual traffic values. In Table 25, each diagonal matrix entry represents intrasite call usage, and all other entries represent intersite call usage. The call usages used to populate the table can be determined empirically or through theoretical means. In some cases, actual call usage data can be obtained through polling an existing system. In other cases, it might be appropriate to apply a mathematical model to estimate the call usages.

Table 25: 3-site standalone community of interest (COI) matrix

CUR	To endpoints in site __		
	1	**2**	**3**
From endpoints in Site __ **1**	Call usage generated by Site 1 endpoints, terminating at Site 1 endpoints	Call usage generated by Site 1 endpoints, terminating at Site 2 endpoints	Call usage generated by Site 1 endpoints, terminating at Site 3 endpoints
2	Call usage generated by Site 2 endpoints, terminating at Site 1 endpoints	Call usage generated by Site 2 endpoints, terminating at Site 2 endpoints	Call usage generated by Site 2 endpoints, terminating at Site 3 endpoints
3	Call usage generated by Site 3 endpoints, terminating at Site 1 endpoints	Call usage generated by Site 3 endpoints, terminating at Site 2 endpoints	Call usage generated by Site 3 stations, terminating at Site 3 endpoints

One of the first steps in the process is to distinguish between intercom call usage, inbound PSTN call usage, and outbound PSTN call usage. Inbound and outbound tie trunk usage must also be considered when working with multiple Communication Manager systems that networked together. However, that discussion is presented in a later section.

Although Avaya systems can be used as tandem switches for PSTN traffic, that possibility is not considered here. Traffic between two other Avaya systems in a network is the only traffic that can be routed through Communication Manager. So, in the case of a single stand-alone system, there is typically no tandem traffic. Therefore, because every call involves at least one station, one must be careful to reconcile the station usage with the call usage.

For example, suppose that the total station usage is 100 Erlangs, which could hypothetically correspond to 20 Erlangs of intercom call usage, 30 Erlangs of inbound PSTN usage, and 30 Erlangs of outbound PSTN usage:

- **Intercom** station usage = 40 Erlangs (2 Avaya stations per call x 20 Erlangs of intercom call usage)
- **Inbound** station usage = 30 Erlangs (1 Avaya station per call x 30 Erlangs of inbound call usage)
- **Outbound** station usage = 30 Erlangs (1 Avaya station per call x 30 Erlangs of outbound call usage)

The 40 Erlangs that are associated with intercom calls, plus the 30 Erlangs that are associated with inbound calls, plus the 30 Erlangs that are associated with outbound calls total 100 Erlangs of station usage.

Alternatively, 100 Erlangs of total station usage could also hypothetically correspond to 35 Erlangs of intercom call usage, 10 Erlangs of inbound PSTN usage, and 20 Erlangs of outbound PSTN usage. Using the procedure from the preceding example to verify this:

- **Intercom** station usage = 70 Erlangs (2 Avaya stations per call x 35 Erlangs of intercom call usage)
- **Inbound** station usage = 10 Erlangs (1 Avaya station per call x 10 Erlangs of inbound call usage)
- **Outbound** station usage = 20 Erlangs (1 Avaya station per call x 20 Erlangs of outbound call usage)

The 70 Erlangs that are associated with intercom calls, plus the 10 Erlangs that are associated with inbound calls, plus the 20 Erlangs that are associated with outbound calls total 100 Erlangs of station usage.

However, suppose that once again the station usage is 100 Erlangs. Assuming that there is no tandem traffic, this cannot correspond to 10 Erlangs of intercom call usage, 20 Erlangs of inbound PSTN usage, and 30 Erlangs of outbound PSTN usage.

- **Intercom** station usage = 20 Erlangs (2 Avaya stations per call x 10 Erlangs of intercom call usage)
- **Inbound** station usage = 20 Erlangs (1 Avaya station per call x 20 Erlangs of inbound call usage)
- **Outbound** station usage = 30 Erlangs (1 Avaya station per call x 30 Erlangs of outbound call usage)

The 20 Erlangs that are associated with intercom calls, plus the 20 Erlangs that are associated with inbound calls, plus the 30 Erlangs that are associated with outbound calls total 70 Erlangs, leaving 30 Erlangs of unaccounted station usage. This is a sign that the parsing of call traffic into intercom, inbound, and outbound might have been done erroneously. One possible explanation for the extra 30 Erlangs of station usage is adjunct traffic, such as stations that are connected to voice mail, providing that 30 Erlangs of voice mail calls makes sense in the model.

The bottom line is, regardless of what model is used to parse call traffic into its various components, one must be able to reconcile the overall station usage with the overall call usage. Specifically, if there is no tandem traffic, the following relationship must hold:

$$\text{SUR} = (2 \times \text{intercom CUR}) + \text{inbound PSTN CUR} + \text{outbound PSTN CUR}$$

Having established that point, several examples describe some methods for populating the COI matrix. For the sake of continuity, all of the examples are built upon Example 1: Station usage.

Example 2: Uniform Distribution model

In the case of a stand-alone Avaya system, the Uniform Distribution model works on the assumption that when a given station places an intercom call, the call is equally likely to terminate at any of the other stations in the entire system. Analogous statements regarding this model can also be made for inbound trunk calls and outbound trunk calls. Specifically, any inbound call is equally likely to terminate at any of the stations in the system, and any outbound call is equally likely to have been originated by any of the stations in the system. The fundamental concept underlying the Uniform Distribution model is that stations are essentially indistinguishable from one another from a traffic engineering point of view. This model is usually the most appropriate option when engineering a system for which little or no information about the nature of the various stations exists. This model will now be applied to the system that is described in Example 1: Station usage.

The design criteria for Example 1: Station usage was one-third of all calls being intercom, one-third being inbound PSTN, and one-third being outbound PSTN. From the station usages that are listed in Example 1: Station usage, it follows that the total station usage in Atlanta is 195 Erlangs, the total in Boston is 72 Erlangs, and the total in Cleveland is 34 Erlangs, for a system-wide total of 301 Erlangs of station usage. Under the “one-third intercom, one-third inbound, one-third outbound” assumption, this corresponds to a system-wide total of 75 Erlangs of intercom call usage, 75 Erlangs of inbound call usage, and 75 Erlangs of outbound call usage (rounding to the nearest Erlang in each case). To verify this, first consider the fact that all three components are equal (each is 75 Erlangs) satisfies the “one-third, one-third, one-third” requirement. Furthermore, since 75 Erlangs of intercom call usage corresponds to 150 Erlangs of station usage, 75 Erlangs of inbound call usage corresponds to 75 Erlangs of station usage, and 75 Erlangs of outbound call usage corresponds to 75 Erlangs of station usage, there is a total of 150 + 75 + 75 = 300 Erlangs of station usage. This agrees with the specified 301 Erlangs if one ignores error due to rounding off.

One could assume in this example that each PSTN trunk is capable of carrying both inbound calls and outbound calls. Trunks are normally engineered to a desired Grade of Service (GOS), or blocking level. A commonly used GOS for trunks is P01, which represents a nominal blocking rate of 1 out of every 100 call attempts. To determine how many trunks are needed to attain P01, one must know the call traffic load to be carried by those trunks. Both inbound call usage and outbound call usage are included in that load.

Note:

If IP Softphone telecommuters were used in this example, they would have also contributed toward trunk load. Although the signaling link between a telecommuter and the Communication Manager system to which the telecommuter is registered is carried over IP, the media flow between the two uses a PSTN trunk.

Example 1: Station usage indicates that the total load to be carried by the trunks is 75 + 75 = 150 Erlangs, which accounts for both inbound and outbound PSTN call usage. Use of the standard Erlang blocking model indicates that 171 trunks (DS0s) would be required to carry the 150 Erlangs of trunk call usage at P01. However, one must consider the trunk selection process for PSTN calls.

Communication Manager uses a first-site-preference algorithm for outbound trunk calls. This algorithm specifies that all outbound calls first attempt to seize a trunk within the originating station's site, and tries to use a trunk in a different site if and only if it is blocked at its local trunks. For inbound PSTN trunk calls, the CO selects the trunk. Therefore, Communication Manager cannot use an analogous first-site-preference algorithm for inbound calls. However, such an algorithm can be effectively imposed by assigning different calling numbers for the three sites, which is typical in this example since the sites are in different area codes.

The goal of a first-site preference algorithm is to minimize intersite traffic. When this algorithm is used, there is intersite traffic if and only if it overflows to a trunk on another site after having been blocked at the trunks in its own site. Under the assumption that a first-site preference algorithm is used in this example, the trunks at the three individual sites must be sized independently, as opposed to all together. Initially, the overflow traffic is ignored, but that topic is discussed later in this example.

Since overflow traffic is ignored for the time being, intersite trunk traffic is zero, which implies that the off-diagonal entries of the inbound and outbound COI matrices will all be zero. To determine the values of the diagonal entries, which correspond to intrasite trunk usage, the Uniform Distribution model is applied. In particular, 65% (that is, 1755/2709) of the stations are in Atlanta, 24% (that is, 648/2709) of the stations are in Boston, and 11% (that is, 306/2709) of the stations are in Cleveland. Therefore, the Uniform Distribution model implies that 65% of the 75 Erlangs of inbound CUR (that is, 49 Erlangs) is assumed to terminate in Site 1 (Atlanta), 24% (that is, 18 Erlangs) is assumed to terminate in Site 2 (Boston), and 11% (that is, 8 Erlangs) is assumed to terminate in Site 3 (Cleveland). Similarly, 49 Erlangs of outbound CUR is assumed to originate in Site 1, 18 Erlangs is assumed to originate in Site 2, and 8 Erlangs is assumed to originate in Site 3.

It is instructive for this example to construct three different COI matrices rather than just one. Specifically, it is useful to construct one for intercom CUR, one for inbound CUR, and one for outbound CUR. The information from the previous paragraph can be used to populate the following inbound and outbound COI matrices (Table 26: Inbound COI matrix for the Uniform Distribution model in Example 2: Uniform Distribution model on page 187):

Table 26: Inbound COI matrix for the Uniform Distribution model in Example 2: Uniform Distribution model

Inbound CUR		To stations in Site __		
		1	2	3
From trunks in Site ____	1	49 Erlangs	0	0
	2	0	18 Erlangs	0
	3	0	0	8 Erlangs

Table 27: Outbound COI matrix for Uniform Distribution Model in Example 2: Uniform Distribution model

Outbound CUR		To trunks in Site __		
		1	**2**	**3**
From stations in Site ____	**1**	49 Erlangs	0	0
	2	0	18 Erlangs	0
	3	0	0	8 Erlangs

Again, Table 26 and Table 27 are constructed without considering overflow traffic.These tables imply that the Site 1 PSTN trunks carry 98 Erlangs (49 inbound and 49 outbound) of traffic, the Site 2 trunks carry 36 Erlangs, and the Site 3 trunks carry 16 Erlangs. Applying the standard Erlang loss model with a P01 GOS to each of the three sites implies that at least 116 trunks are needed in Site 1, at least 49 trunks are needed in Site 2, and at least 26 trunks are needed in Site 3. Note that this constitutes a total of 191 trunks, as opposed to the estimate of 171 trunks that was obtained without sizing the three trunk groups separately. A total of 171 could be used to attain an overall grade of service of P01, but that would induce a large amount of intersite traffic. The use of 191 total trunks, distributed between the three sites as specified above, ensures that at least 99% of the calls are guaranteed to be *intrasite*.

In some cases, there might be factors that justify over-engineering the trunk groups. For example, a customer who is based in North America most likely leases T1 trunk facilities between each of its sites and the appropriate COs. In this example, it might be reasonable to use five T1 facilities (that is, 120 DS0 channels) for Atlanta, three T1 facilities (that is, 72 DS0 channels) for Boston, and two T1 facilities (that is, 48 DS0 channels) for Cleveland. This yields an overall GOS much better than P01, and at the same time, the use of standardized equipment reduces costs. In fact, the use of Erlang's loss formula implies a blocking probability of 0.004 in Atlanta, and negligible blocking probabilities (that is, several orders of magnitude better than P01) for the other two sites. These extremely low-blocking probabilities justify the assumption that intersite trunk traffic (overflow traffic) is negligible in this example.

Finally, the entries for the intercom COI matrix must be determined. Of the 195 Erlangs of station usage in that site, 49 Erlangs are associated with inbound calls, and 49 Erlangs are associated with outbound calls. That leaves 195 - 49 - 49 = 97 Erlangs of station usage in the Atlanta site for intercom calls. Similarly, there are 72 - 18 - 18 = 36 Erlangs of station usage in the Boston site for intercom calls, and 34 - 8 - 8 = 18 Erlangs of station usage in the Cleveland site for intercom calls.

It is assumed that half of each individual station's usage is associated with calls that the station generates, and the other half is associated with calls that the station receives. Therefore, half of the 97 Erlangs of station usage (that is, 49 Erlangs) in the Atlanta site corresponds to intercom calls originated in the Atlanta site. Similarly, half of the 36 Erlangs of station usage (that is, 18 Erlangs) in the Boston site corresponds to intercom calls originated in Boston, and half of the 18 Erlangs of station usage (that is, 9 Erlangs) in the Cleveland site corresponds to intercom calls originated in Cleveland.

Using the percentages from earlier, the Uniform Distribution model implies that 65% of the intercom traffic originated by each station in Atlanta is terminated in Atlanta, 24% is terminated in Boston, and 11% is terminated in Cleveland. Applying those percentages to the 49 Erlangs of intercom traffic that is generated in Atlanta implies that 32 Erlangs of intercom call usage is generated in Atlanta for termination in Atlanta, 12 Erlangs of intercom call usage is generated in Atlanta for termination in Boston, and 5 Erlangs of intercom call usage is generated in Atlanta for termination in Cleveland. Analogous calculations can be made in relation to intercom traffic that is generated in Boston and in Cleveland. The results are tabulated in the intercom COI matrix that is associated with this example (Table 28: Intercom COI matrix for the Uniform Distribution model in Example 2: Uniform Distribution model on page 189):

Table 28: Intercom COI matrix for the Uniform Distribution model in Example 2: Uniform Distribution model

Intercom CUR		To stations in Site __ (all data in Erlangs)		
		1	**2**	**3**
From stations in Site ____	**1**	32	12	5
	2	12	4	2
	3	6	2	1

The general formulas used to populate the COI matrix entries in Table 26, Table 27, and Table 28, respectively, for the Uniform Distribution model are:

$$\text{Inbound CUR to Site } i = \left(\frac{\text{number of stations in Site } i}{\text{total number of stations}}\right) \times (\text{total inbound CUR})$$

$$\text{Outbound CUR from Site } i = \left(\frac{\text{number of stations in Site } i}{\text{total number of stations}}\right) \times (\text{total outbound CUR})$$

$$\text{Intercom CUR from Site } i \text{ to Site } j = \left(\frac{\text{number of stations in Site } j}{\text{total number of stations}}\right) \times \begin{pmatrix}\text{total intercom CUR} \\ \text{originating in Site } i\end{pmatrix}$$

Additional comments regarding Example 2: Uniform Distribution model

In the Uniform Distribution model introduced in Example 2: Uniform Distribution model on page 186, the relative weights that are associated with the various sites correspond to the distribution of stations throughout the sites. Alternatively, the weights could correspond to the relative overall station usages in the various sites. Such a model takes into account not only the number of stations, but also how busy the stations are. In Example 2: Uniform Distribution model, since every station is assumed to have the same usage (specifically, 0.11 Erlangs), the weights that are based on the number of stations per site are exactly the same as the weights that are based on the overall station usage per site. Such a model is not always appropriate. For example, consider a system with two sites, with 100 stations in each site. Suppose that the average usage per station in Site 1 is 0.1 Erlangs, and that the average usage per station in Site 2 is 0.2 Erlangs. In a Uniform Distribution model where the weights are based on station usage per endpoint, a caller in Site 1 is twice as likely to call a station in Site 2 than a station in Site 1 (because the total station usage in Site 2 is 20 Erlangs, and the total station usage in Site 1 is only 10 Erlangs). The general formulas used to populate the COI matrix entries in Table 26,

Table 27, and Table 28, respectively, for the Uniform Distribution model based on relative SUR are:

$$\text{Inbound CUR to Site } i = \left(\frac{\text{total station usage in Site } i}{\text{total station usage}}\right) \times (\text{total inbound CUR})$$

$$\text{Outbound CUR from Site } i = \left(\frac{\text{total station usage in Site } i}{\text{total station usage}}\right) \times (\text{total outbound CUR})$$

$$\text{Intercom CUR from Site } i \text{ to Site } j = \left(\frac{\text{total station usage in Site } j}{\text{total station usage}}\right) \times \left(\begin{matrix}\text{total intercom CUR} \\ \text{originating in Site } i\end{matrix}\right)$$

Example 3: Empirical approach for existing systems

Another possible means of populating the COI matrices exists for established systems. In such cases, the necessary information can be read from traffic reports. This method is particularly useful for customers who are considering an upgrade from their current equipment.

Expanded COI matrices

So far, all the discussion pertaining to COI matrices has focused on a macroscopic view of sites. In particular, all the COI matrices presented have dedicated one cell for each pair of sites. In preparation for Resource sizing on page 198, it is useful to partition each such cell into collections of smaller cells that describe the call flows between different communities of endpoint types within the sites.

One possible partitioning scheme for each site is to create the following three general endpoint categories:

- IP endpoints
- Circuit-switched endpoints
- PSTN trunks

Consider the COI matrix for a three-site, stand-alone Communication Manager system, as presented in Table 25. A suitable expansion of that matrix might take the form of the matrix in Table 29: Expanded COI matrix for a three-site system on page 192 in which

- **I** represents IP endpoints
- **C** represents circuit-switched endpoints
- **P** represents PSTN trunks

This finer categorization of endpoints permits the use of a single COI matrix for intercom, inbound, and outbound call usage rates.

Table 29: Expanded COI matrix for a three-site system

			To endpoints in Site ___								
			1			2			3		
			I	C	P	I	C	P	I	C	P
From endpoints in Site ___	1	I									
		C									
		P									
	2	I									
		C									
		P									
	3	I									
		C									
		P									

Example 4: Expanded COI matrices

In this example, we revisit Example 2: Uniform Distribution model, which pertains to the Uniform Distribution model, in more detail. The various endpoints are grouped into the three categories that are referenced in Table 29. The COI matrix in Table 28 lists the intercom call usage rates between each pair of sites, including intrasite call usage. Those usage rates can be broken down into finer components. Table 30: Endpoints in a three-site system on page 193 reviews the various endpoints in each site.

Table 30: Endpoints in a three-site system

Endpoints	Atlanta	Boston	Cleveland
IP stations	1107 (1080 IP Telephones + 27 Road Warriors)	450 (450 IP Telephones)	270 (270 IP Telephones)
Circuit-switched stations	648 (540 DCP stations + 108 analog stations)	198 (180 DCP stations + 18 analog stations)	36 (36 analog stations)
PSTN trunks	120 (DS0) PSTN Trunks (5 T1 facilities)	48 (DS0) PSTN Trunks (2 T1 facilities)	24 (DS0) PSTN Trunks (1 T1 facility)

First consider the 32 Erlangs of intercom CUR between Site 1 stations (Table 28). Site 1 (Atlanta) has a total of 1755 stations, 1107 of which are IP stations, and 648 of which are circuit-switched stations. So, 63% of the stations in Site 1 are IP, and 37% are circuit switched. Therefore, 63% of Site 1 intercom calls are generated by IP stations, and 63% of those calls are terminated by IP stations. Since 63% of 63% is 39.7%, 39.7% of Site 1 intercom calls are IP station to IP station. Similarly, 37% of the Site 1 intercom calls that are generated by IP stations are terminated by circuit-switched stations. Since 37% of 63% is 23.3%, 23.3% of Site 1 intercom calls are IP station to circuit-switched station.

Also, 37% of Site 1 intercom calls are generated by circuit-switched stations, and 63% of those calls are terminated by IP stations. Since 63% of 37% is 23.3%, 23.3% of Site 1 intercom calls are circuit-switched station to IP station. Finally, 37% of the Site 1 intercom calls that are generated by circuit-switched stations are terminated by circuit-switched stations. Since 37% of 37% is 13.7%, 13.7% of Site 1 intercom calls are circuit-switched station to circuit-switched station.

So, since 39.7% of Site 1 intercom calls are IP station to IP station, IP station to IP station call usage is 39.7% of the 32 Erlangs of overall Site 1 intercom CUR, or 12.7 Erlangs. Similarly, both the Site 1 IP station to circuit-switched station CUR and the Site 1 circuit-switched station to IP station CUR are equal to 23.3% of 32 Erlangs, or 7.5 Erlangs. Finally, the Site 1 circuit-switched station to circuit-switched station CUR is 13.7% of 32 Erlangs, or 4.4 Erlangs.

A similar process is used to break down the 12 Erlangs of intercom CUR into its components. There are a total of 648 stations in Site 2 (Atlanta), 450 of which are IP stations, and 198 of which are circuit-switched stations. So, 69% of the stations in Site 2 are IP, and 31% are circuit-switched. We have already determined that 63% of intercom calls that are generated in Site 1 are generated by IP stations. Similarly, 69% of intercom calls that are terminated in Site 2 are terminated by IP stations. Since 69% of 63% is 43.5%, 43.5% of Site 1 to Site 2 intercom calls are IP station to IP station. Also, 31% of intercom calls that are terminated in Site 2 are terminated by circuit-switched stations. Since 31% of 63% is 19.5%, 19.5% of Site 1 to Site 2 intercom calls are IP station to circuit-switched station.

In addition, 37% of intercom calls that are generated in Site 1 are generated by circuit-switched stations, and 69% of those calls are terminated by IP stations. Since 69% of 37% is 25.5%, 25.5% of Site 1 to Site 2 intercom calls are circuit-switched station to IP station. Finally, 37% of intercom calls that are generated in Site 1 are generated by circuit-switched stations, and 31% of those calls are terminated by circuit-switched stations. Since 31% of 37% is 11.5%, 11.5% of Site 1 to Site 2 intercom calls are circuit-switched station to circuit-switched station.

So, since 43.5% of Site 1 to Site 2 intercom calls are IP station to IP station, Site 1 IP station to Site 2 IP station CUR is 43.5% of the 12 Erlangs of overall Site 1 to Site 2 intercom CUR, or 5.2 Erlangs. Similarly, the Site 1 IP station to Site 2 circuit-switched station CUR is equal to 19.5% of 12 Erlangs, or 2.3 Erlangs, and the Site 1 circuit-switched station to Site 2 IP station CUR is equal to 25.5% of 12 Erlangs, or 3.1 Erlangs. Finally, the Site 1 circuit-switched station to Site 2 circuit-switched station CUR is 11.5% of 12 Erlangs, or 1.4 Erlangs.

The values for the remaining COI cells that correspond to intercom traffic for this example are calculated in a similar manner. Table 31: COI matrix for Example 4: Expanded COI matrices (intercom CUR values only) summarizes the results of that exercise:

Table 31: COI matrix for Example 4: Expanded COI matrices (intercom CUR values only)

			To endpoints in site ___								
			1			2			3		
			I	C	P	I	C	P	I	C	P
From endpoints in site ___	1	I	12.7	7.5		5.2	2.3		2.8	0.37	
		C	7.5	4.4		3.1	1.4		1.6	0.22	
		P									
	2	I	5.2	3.1		1.9	0.85		1.2	0.16	
		C	2.3	1.4		0.85	0.37		0.54	0.07	
		P									
	3	I	2.8	1.6		1.2	0.54		0.78	0.10	
		C	0.37	0.22		0.16	0.07		0.10	0.01	
		P									

The general formula that is used to determine the expanded intercom CUR entries in Table 31 is:

$$\begin{array}{l}\text{CUR generated by stations of type } t \text{ in Site } i \\ \text{and terminated by stations of type } t \text{ in Site } j\end{array} = f_{\mathrm{i}}{}^{t} \times f_{\mathrm{j}}{}^{t} \times (\text{intercom CUR from Site } i \text{ to Site } j\ )$$

where:

- "Type *t*" refers to IP or circuit-switched
- $f_{\mathrm{i}}{}^{t} = \dfrac{\text{number of type } t \text{ stations in Site } i}{\text{total number of stations in Site } i}$
- $f_{\mathrm{j}}{}^{t} = \dfrac{\text{number of type } t \text{ stations in Site } j}{\text{total number of stations in Site } j}$

Now that the intercom CURs have been determined, CURs that involve trunks will be addressed. First, because Communication Manager systems are rarely used to route PSTN traffic, all of the COI matrix entries that correspond to PSTN-PSTN traffic are zero. Next, Table 26 and Table 27 help us determine the entries that correspond to inbound and outbound PSTN traffic.

According to Table 26, the inbound PSTN usage that arrives on Site 1 trunks and terminates at Site 1 stations is 49 Erlangs. We have already determined that 63% of the stations in Site 1 are IP and 37% are circuit switched. Therefore, the Uniform Distribution model implies that 63% of the 49 Erlangs (that is, 30.9 Erlangs) is inbound to Site 1 IP stations, and 37% of the 49 Erlangs (that is, 18.1 Erlangs) is inbound to Site 1 circuit-switched stations. Similarly, the Uniform Distribution model and Table 27 together imply that 63% of the 49 Erlangs of Site 1 outbound PSTN usage (that is, 30.9 Erlangs) is outbound from Site 1 IP stations through Site 1 PSTN trunks, and 37% (that is, 18.1 Erlangs) is outbound from Site 1 circuit-switched stations through Site 1 PSTN trunks. Note that by an assumption in Example 2: Uniform Distribution model, Site 1 inbound and outbound traffic only terminates and originates at Site 1 stations. This completes the work for Site 1. Sites 2 and 3 are handled in a similar manner, and the resulting completed COI matrix for Example 4: Expanded COI matrices is provided in Table 32: Completed COI matrix for Example 4: Expanded COI matrices on page 196.

Table 32: Completed COI matrix for Example 4: Expanded COI matrices

			To endpoints in Site ___								
			1			2			3		
			I	C	P	I	C	P	I	C	P
From endpoints in Site ___	1	I	12.7	7.5	0	5.2	2.3	0	2.8	0.37	0
		C	7.5	4.4	0	3.1	1.4	0	1.6	0.22	0
		P	30.9	18.1	0	0	0	0	0	0	0
	2	I	5.2	3.1	0	1.9	0.85	0	1.2	0.16	0
		C	2.3	1.4	0	0.85	0.37	0	0.54	0.07	0
		P	0	0	0	12.5	5.5	0	0	0	0
	3	I	2.8	1.6	0	1.2	0.54	0	0.78	0.10	0
		C	0.37	0.22	0	0.16	0.07	0	0.10	0.01	0
		P	0	0	0	0	0	0	7.1	0.94	0

The general formula that is used to determine the expanded inbound and outbound CUR entries in Table 32 is:

$$\text{Inbound CUR to stations of type } t \text{ in Site } j \text{ over PSTN trunks in Site } i = f_j^{\,t} \times \left(\begin{array}{c} \text{inbound CUR from trunks in Site } i \\ \text{to stations in Site } j \end{array} \right)$$

$$\text{Outbound CUR from stations of type } t \text{ in Site } i \text{ over PSTN trunks in Site } j = f_i^{\,t} \times \left(\begin{array}{c} \text{outbound CUR from stations in Site } i \\ \text{to trunks in Site } j \end{array} \right)$$

where:

- "Type *t*" refers to IP or circuit-switched
- $f_i^{\,t} = \dfrac{\text{number of type } t \text{ stations in Site } i}{\text{total number of stations in Site } i}$
- $f_j^{\,t} = \dfrac{\text{number of type } t \text{ stations in Site } j}{\text{total number of stations in Site } j}$

In general, one may choose to expand a COI matrix in any of several different possible ways, depending upon the needs of the problem. In the preceding example, separating the endpoints into IP, circuit-switched, and PSTN makes sense for the upcoming resource-sizing calculations, as will be seen later in this document. In other examples, other sets of categories may be more appropriate. Also, the number of categories per site is not limited to three.

COIs for multiple-site networks

The discussion of COIs up to this point has been limited to stand-alone Communication Manager systems. It is also possible to network several Communication Manager systems together. IP tie trunks serve as the most common mode of interconnectivity. However, circuit-switched tie trunks are also supported.

To engineer a network of multiple Communication Manager systems, one must to know the topology of sites within each of the individual systems, and the overall topology of the entire configuration. Consider the network of systems that Figure 64: Network of Avaya systems and system sites on page 197 shows.

Figure 64: Network of Avaya systems and system sites

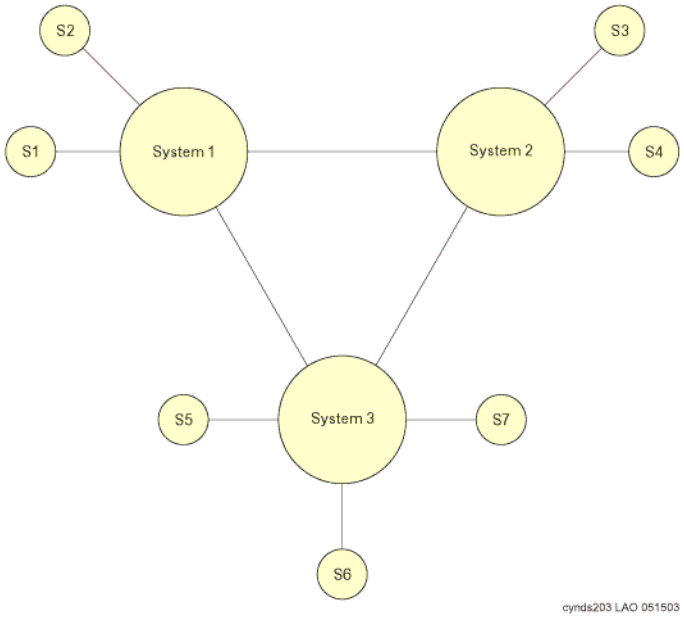


Figure 64 shows three distinct Communication Manager systems, that are interconnected by IP trunk groups. This network has a total of seven sites, which are labeled “S1” through “S7” in the figure. Systems 1 and 2 each have two sites, and System 3 has three sites.

A seven-site COI matrix analogous to the three-site matrix in Table 25: 3-site standalone community of interest (COI) matrix on page 184 can be constructed for the network shown in Figure 64. A corresponding seven-site, expanded COI matrix, similar to the one in Table 29: Expanded COI matrix for a three-site system on page 192, can also be constructed. However, when multiple systems are networked together, the additional step of engineering the tie trunk groups must be performed. To do this, the COI matrices are used to determine the traffic flow between each pair of Avaya systems.

In the network that is shown in Figure 64, IP Trunk Group 1 carries calls between Sites 1 and 3, Sites 1 and 4, Sites 2 and 3, and Sites 2 and 4, in addition to a presumably small amount of overflow traffic that involves other sites. The traffic load that is associated with such calls is used to size that trunk group. Tie trunk groups are typically sized at either P01 (1% blocking) or P03 (3% blocking). In a system such as the one in Figure 64, the traffic engineer must account for overflow traffic. The traditional Wilkinson model is an effective tool for doing so. However, for systems that have larger numbers of systems in the network, there can be many possible paths between a given pair of systems. In such cases, determining the hierarchy of paths to consider for calls between two systems is not always straightforward. The analysis involved in sizing the tie trunk groups in topologies such as those can be quite complex.

Resource sizing

This section provides a description of the resources that have the potential to be bottlenecks, and a discussion about how to engineer them. This is the final stage of the design process.

Overview

The primary Communication Manager resources that have the potential to be bottlenecks are:

- the TN799DP C-LAN (Control LAN) circuit packs
- the port network TDM bus pairs
- the TN2602AP IP Media Resource 320 and TN2302AP IP Media Processor circuit packs
- the TN2312BP IP server (IPSI) circuit packs
- the server’s processing capacity
- IP bandwidth.

Signaling resources

The TN799DP C-LAN and the TN2312BP (IPSI) circuit packs are the primary signaling traffic bearing components residing within a port network. Both have finite internal resources such as sockets and data-link connection identifiers (DLCIs) for assignment to and use by endpoints. In addition, both components, being circuit packs, have firmware running on processors with finite capacities to process signaling traffic. Therefore resource sizing the IPSI and the C-LAN involves both tracking the sockets/DLCIs and the signaling traffic throughput.

The TN799DP C-LAN circuit pack provides the interface for a signaling channel between an IP endpoint and a packet bus (which ultimately interfaces with the Avaya server). When an IP endpoint, G250 MG, G350 MG, or G700 MG registers to a C-LAN circuit pack, it allocates a TCP socket dedicated to that endpoint or gateway, for as long as it remains registered. C-LAN sockets are also required for the support of certain adjuncts.

Each C-LAN circuit pack has a finite number of C-LAN sockets. The total number of C-LAN circuit packs that are required to support a particular system depends on the total required number of C-LAN sockets, which in turn depends on the total number of IP endpoints, G250/G350/G700 MGs, and adjuncts. An individual C-LAN circuit pack can support endpoints in different Network Regions, even those that are not administered to communicate with each other.

Sizing the TN2312BP IPSI circuit packs is a fairly straightforward process. The number of IPSI circuit packs that are required in the system depends on the total number of C-LAN sockets that are required, and the number of ISDN D-channels in the system. Specifically, each IPSI circuit pack supports up to a combined total of 2,480 C-LAN sockets and ISDN D-channels. This is a system-wide constraint, as opposed to a site-by-site constraint. For an IP-PNC system, each PN must house exactly one IPSI circuit pack, neglecting duplicated IPSI circuit packs for enhanced reliability. Therefore, if the C-LAN sockets and the ISDN D-channels indicate a need for more IPSI circuit packs than the required number of PNs to support the TDM usage, more PNs are needed (note that placing two active IPSI circuit packs in a single PN is not permitted). In other words, the number of PNs must be large enough to fulfill both the TDM and the IPSI requirements.

In a system utilizing a circuit-switched center stage an IPSI circuit pack is not required in each port network. However, there are restrictions pertaining to how many port networks can be supported by a single IPSI circuit pack.

If the number of port networks needs to be increased to satisfy the IPSI requirements, then the TDM and media processing engineering processes must be redone (since an increased number of port networks implies an increase in inter-port-network traffic). This is an iterative process.

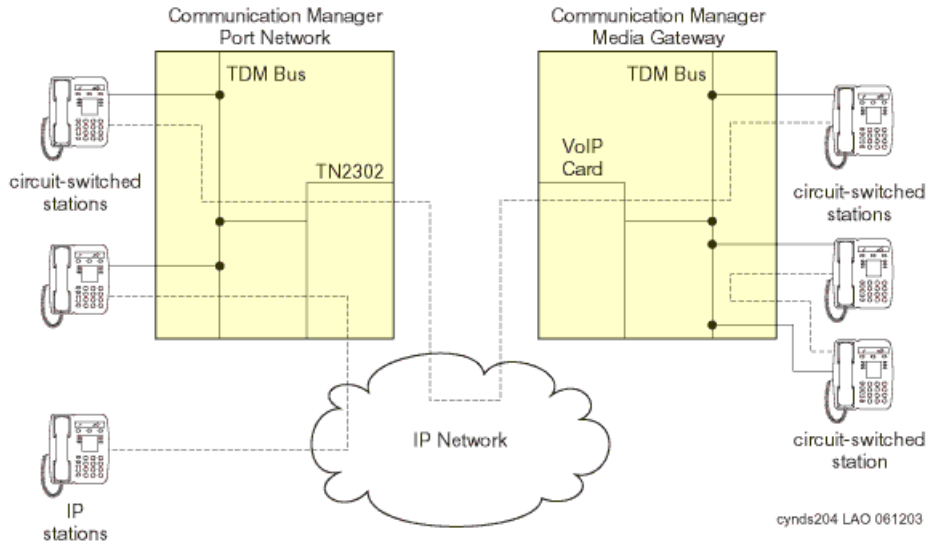
In addition to counting sockets and DLCIs in allocating C-LANs and IPSIs, a separate, independent traffic engineering process involves modeling the signaling message traffic through them. The rate of message traffic depends primarily on the call traffic at the endpoints and MGs signaling through the sockets/DLCIs. Each call generates a certain amount of messages between the endpoints and the server. The exact number and sizes of the messages depends on the protocols involved. Combining the messages per call with a call rate gives estimates of

the message traffic through C-LANs and IPSIs. Optimal configurations allocate enough of both to maintain traffic levels at or below known stable thresholds. Avaya configuration software tools perform the requisite analysis and resulting resource sizing, as needed.

Media processing and TDM resources

The media processing resources on the TN2302AP IP Media Processor and/or TN2602AP IP Media Resource 320 circuit packs on a PN or a G650 Media Gateway provide the gateway for an audio channel between an IP endpoint and a circuit-switched TDM bus. On a G350 or G700 Media Gateway, the media processing resources reside on an on-board VoIP module. A G700 Media Gateway can accommodate an optional extra VoIP module as well. The media stream for a call between a circuit-switched endpoint and an IP endpoint on a PN or MG traverses the PN's or MG's TDM bus, a TN2302AP or TN2602AP media processing circuit pack or a VoIP module (as applicable), and an IP network. The media stream for a call between two circuit-switched endpoints on a single port network or Media Gateway uses that PN or Media Gateway's TDM bus, and does not require any media processing resources. However, the media stream for a call between two circuit-switched endpoints that reside on different circuit-switched facilities (that is, two different PNs, two different Media Gateways, or one PN and one Media Gateway) traverses each circuit-switched facility's TDM bus, a media processing resource on each circuit-switched facility (a Media Processing circuit pack or VoIP Media Module, as applicable), and an IP network. Figure 65: Examples of media streams between Avaya endpoints on page 200 shows some examples of the various possible media streams.

Figure 65: Examples of media streams between Avaya endpoints



Although we stated that calls between two circuit-switched endpoints on different port networks use an IP connection, the use of a circuit-switched center stage between the two PNs is also supported. However, using circuit-switched facilities is not viable for interconnecting multiple Media Gateways, or for interconnecting PNs and Media Gateways.

Figure 65 provides some insight into how a call between an IP endpoint and a circuit-switched endpoint, as well as a call between two circuit-switched endpoints, utilizes media processing and TDM resources. Calls between IP endpoints are addressed first.

Communication Manager supports three general modes of connectivity between IP endpoints: *IP-TDM-IP* connectivity, *hairpinning*, and *shuffling*. Hairpinning can take one of two forms: *deep* or *shallow*. These various modes of connectivity are described in more detail below.

IP-TDM-IP connectivity

A call that uses IP-TDM-IP connectivity between two IP endpoints requires one bidirectional media processing “channel” for each IP endpoint involved, as well as a bidirectional TDM resource on every PN (or Media Gateway) that is involved in the call. This option most often applies in systems that use a circuit-switched center stage for interport network connectivity. In such a system, IP-TDM-IP is required in order for two IP endpoints in network regions not configured for connectivity (in the sense of the IRCM matrix) to talk to one another.

Hairpinning

Unlike the IP-TDM-IP connectivity option, hairpinning requires that all media processing resources for a given call reside on a single TN2302AP or TN2602AP media processing circuit pack or a single G350 or G700 Media Gateway VoIP Media Module. A hairpinned call is originally set up as an IP-TDM-IP call, but once the set-up process is complete, no TDM resources are required. However, resources on the Media Processing circuit pack or VoIP Media Module are required for the duration of the call. A Media Processing circuit pack and a VoIP Media Module each house an onboard Central Processing Unit (CPU) and Digital Signal Processors (DSPs).

Shuffling

A shuffled call relinquishes all TDM and media processing resources after call setup. Therefore, the media stream of a shuffled call traverses only an IP network. This is the most commonly used mode of connectivity between two IP endpoints in the same system.

Figure 66: Connectivity modes between two IP endpoints on page 202 shows the various modes of connectivity between two IP endpoints.

Figure 66: Connectivity modes between two IP endpoints

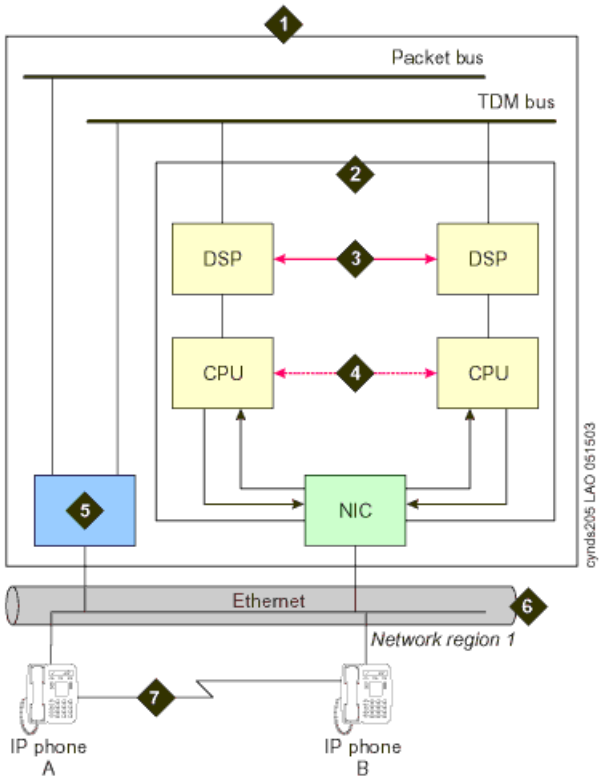


Figure notes:

1. **Avaya server**
2. **TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 (Media Processor board)**
3. **Deep hairpinned audio connection**
4. **Shallow hairpinned audio connection**
5. **TN799DP Control LAN (C-LAN) circuit pack**
6. **Customer LAN**
7. **Shuffled audio connection**

At this point, we can quantify the TDM and media processing requirements for various call types. Throughout this discussion, calls between two IP stations are assumed to use shuffling. That being the case, an intrasite call between two IP endpoints requires neither TDM nor media processing resources, beyond the completion of the initial call set-up process. Each intrasite call between an IP endpoint and a circuit-switched endpoint (including PSTN trunks) requires one TDM resource and one media processing resource. Each of these resources is furnished by the PN or the Media Gateway to which the circuit-switched endpoint is administered. See Figure 65: Examples of media streams between Avaya endpoints on page 200 for an example.

The TDM and media processing resources that are required for each intrasite call between two circuit-switched endpoints depends upon whether the call is intraport network or interport network. Specifically, each intraport network call requires one TDM resource (on the port network to which the two circuit-switched endpoints are administered), and no media processing resources. See Figure 65 for an example. Also, assuming that IP interport network

connectivity is being used (as opposed to a center stage), each interport network call requires two TDM resources and two media processing resources. One of each of these resources is supplied by each of the PNs that is involved in the call. In the preceding discussion, everything that applies to a PN also applies to a Media Gateway.

In general, the TDM and media processing requirements for intersite calls are accounted for somewhat differently than the requirements for intrasite calls. Throughout this discussion, we assume that shuffling is implemented. When an IP endpoint is involved in an intersite call, it induces no TDM or media processing usage in its own site beyond the resources that are initially required for the call set-up process, regardless of the nature of the far-end party. On the other hand, when a circuit-switched endpoint (including PSTN trunks) is involved in an intersite call, one TDM resource and one media processing resource are required from the port network or Media Gateway to which it is administered, regardless of the nature of the far-end party.

The preceding discussion is summarized in Figure 67: Intra-site TDM and Media Processing resource requirements on page 203 and Figure 68: Inter-site TDM and Media Processing resource requirements on page 204.

Figure 67: Intra-site TDM and Media Processing resource requirements

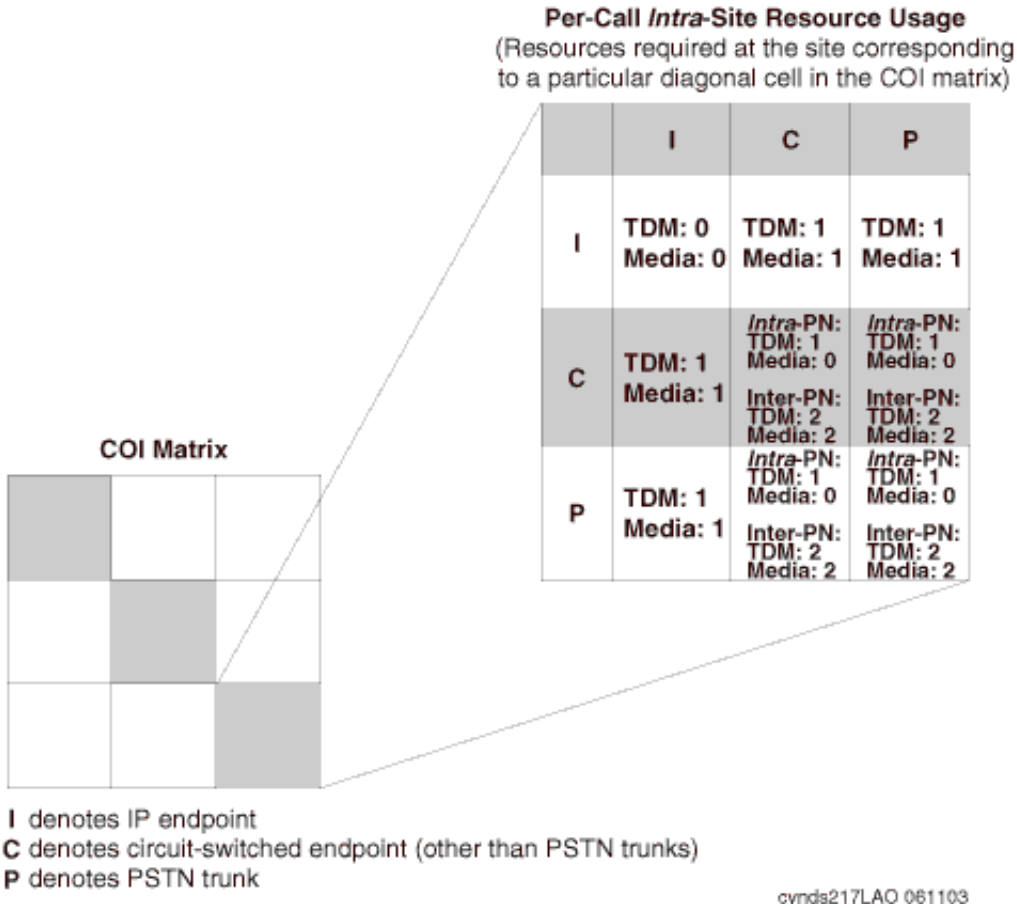
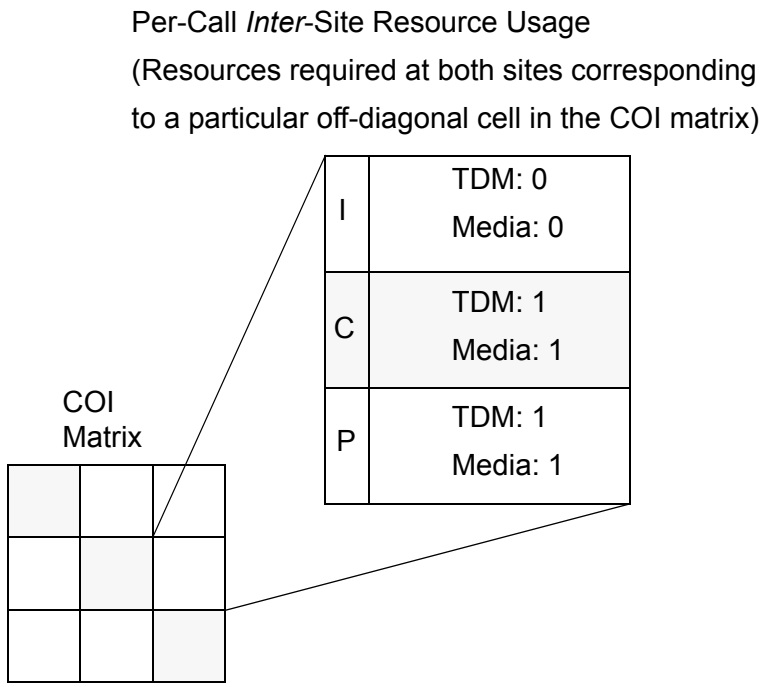


Figure 68: Inter-site TDM and Media Processing resource requirements



In Figure 68, the usages are presented on an endpoint-by-endpoint basis. For example, according to Figure 68, an intersite call between an IP endpoint in Site 1 and a circuit-switched endpoint in Site 2 requires no TDM or media processing resources in Site 1, but does require one TDM resource and one media processing resource in Site 2.

The overall TDM usage and media processing usage for each site can be calculated from an expanded COI matrix, along with the information from Figure 67 and Figure 68. To illustrate, Example 4: Expanded COI matrices will be further expanded.

Example 5: TDM and media processing usage

Consider the COI matrix in Table 32: Completed COI matrix for Example 4: Expanded COI matrices on page 196 in Example 4: Expanded COI matrices. A set of nine cells corresponds to calls originated in Site 1 and terminated in Site 1 (that is, the upper left group of nine cells, arranged in a three-by-three submatrix). The uppermost and leftmost cell of those nine cells indicates that the IP-to-IP call usage for Site 1 intrasite calls is 12.7 Erlangs. The other four cells of those nine cells which fall in a row or column that is labeled “I” indicate that the total call usage between IP endpoints and circuit-switched endpoints (including PSTN trunks) within Site 1 is (7.5 + 30.9 + 7.5 + 30.9) = 76.8 Erlangs. The remaining four cells of those nine cells indicate that the total call usage between two circuit-switched endpoints (including PSTN trunks) within Site 1 is (4.4 + 18.1 + 18.1 + 0) = 40.6 Erlangs. Analogous numbers for intrasite usages that correspond to the other two sites are similarly derived.

Next, consider the three-by-three submatrix that corresponds to calls from Site 1 to Site 2. The total call usage from Site 1 to Site 2 which involves an IP endpoint in Site 1 can be determined by adding the three cell values of those nine cells that correspond to IP endpoints in Site 1. Specifically, the total is (5.2 + 2.3 + 0) = 7.5 Erlangs. The total call usage from Site 1 to Site 2 which involves a circuit-switched endpoint (including PSTN trunks) in Site 1 can be determined by adding the remaining six cell values of those nine. Specifically, that total is (3.1 + 1.4 + 0 + 0 + 0 + 0) = 4.5 Erlangs.

The total call usage from Site 1 to Site 2 which involves an IP endpoint in Site 2 can be determined by adding the three cell values of those nine that correspond to IP endpoints in Site 2. Specifically, the total is (5.2 + 3.1 + 0) = 8.3 Erlangs. And finally, the total call usage from Site 1 to Site 2 which involves a circuit-switched endpoint (including PSTN trunks) in Site 2 can be determined by adding the remaining six cell values of those nine. Specifically, that total is (2.3 + 1.4 + 0 + 0 + 0 + 0) = 3.7 Erlangs. Analogous numbers for the other five combinations of intersite usages are similarly derived. The results are shown in Table 33: Re-categorization of CURs from Table 32 on page 206.

Table 33: Re-categorization of CURs from Table 32

Endpoints		Site 1 (Atlanta)	Site 2 (Boston)	Site 3 (Cleveland)
Intrasite: I, I		12.7 E	1.9 E	0.78 E
Intrasite: I, C or P		76.8 E	26.7 E	14.4 E
Intrasite: C or P, C or P		40.6 E	11.4 E	1.9 E
Calls from Site 1 to Site 2	I	7.5 E	8.3 E	0
	C or P	4.5 E	3.7 E	0
Calls from Site 2 to Site 1	I	7.5 E	8.3 E	0
	C or P	4.5 E	3.7 E	0
Calls from Site 1 to Site 3	I	3.2 E	0	4.4 E
	C or P	1.8 E	0	0.59 E
Calls from Site 3 to Site 1	I	3.2 E	0	4.4 E
	C or P	1.8 E	0	0.59 E
Calls from Site 2 to Site 3	I	0	1.4 E	1.7 E
	C or P	0	0.61 E	0.23 E
Calls from Site 3 to Site 2	I	0	1.4 E	1.7 E
	C or P	0	0.61 E	0.23 E

Table 33 provides a summary of call usage rates, which can be mapped to a table of TDM usage rates and media processing usage rates by using the information in Figure 67 and Figure 68. We assume that there is only one PN in Site 1, one in Site 2, and two G350 Media Gateways in Site 3. Under this assumption, which will be assessed shortly, all calls between circuit-switched endpoints in Sites 1 and 2 are assumed to be intra-Port Network. A minimum of two G350 Media Gateways is required to house the 36 analog telephones in Site 3. The results of this exercise are shown in Table 34: TDM and Media Processing usages (Erlangs) for Example 5: TDM and media processing usage on page 207.

Table 34: TDM and Media Processing usages (Erlangs) for Example 5: TDM and media processing usage

Endpoints		Site 1 (Atlanta)	Site 2 (Boston)	Site 3 (Cleveland)
Intrasite: I, I		TDM: 0 Media: 0	TDM: 0 Media: 0	TDM: 0 Media: 0
Intrasite: I, C or P		TDM: 76.8 Media: 76.8	TDM: 26.7 Media: 26.7	TDM: 14.4 Media: 14.4
Intrasite: C or P, C or P		TDM: 40.6 Media: 0	TDM: 11.4 Media: 0	TDM: 1.9 Media: 0
Calls from Site 1 to Site 2	I	TDM: 0 Media: 0	TDM: 0 Media: 0	TDM: 0 Media: 0
	C or P	TDM: 4.5 Media: 4.5	TDM: 3.7 Media: 3.7	TDM: 0 Media: 0
Calls from Site 2 to Site 1	I	TDM: 0 Media: 0	TDM: 0 Media: 0	TDM: 0 Media: 0
	C or P	TDM: 4.5 Media: 4.5	TDM: 3.7 Media: 3.7	TDM: 0 Media: 0
Calls from Site 1 to Site 3	I	TDM: 0 Media: 0	TDM: 0 Media: 0	TDM: 0 Media: 0
	C or P	TDM: 1.8 Media: 1.8	TDM: 0 Media: 0	TDM: 0.59 Media: 0.59
Calls from Site 3 to Site 1	I	TDM: 0 Media: 0	TDM: 0 Media: 0	TDM: 0 Media: 0
	C or P	TDM: 1.8 Media: 1.8	TDM: 0 Media: 0	TDM: 0.59 Media: 0.59
Calls from Site 2 to Site 3	I	TDM: 0 Media: 0	TDM: 0 Media: 0	TDM: 0 Media: 0
	C or P	TDM: 0 Media: 0	TDM: 0.61 Media: 0.61	TDM: 0.23 Media: 0.23
Calls from Site 3 to Site 2	I	TDM: 0 Media: 0	TDM: 0 Media: 0	TDM: 0 Media: 0
	C or P	TDM: 0 Media: 0	TDM: 0.61 Media: 0.61	TDM: 0.23 Media: 0.23
Totals		TDM: 130.0 Media: 89.4	TDM: 46.7 Media: 35.3	TDM: 17.9 Media: 16.0

The TDM usage rates of 130.0 Erlangs for Site 1 and 46.7 Erlangs for Site 2 can both be easily handled by the TDM facilities of a single PN, which is capable of carrying up to 200 Erlangs of TDM traffic at a P001 GOS. Therefore, the assumption that all calls between two circuit-switched endpoints is intra-Port Network is valid. If one PN was insufficient to support the TDM usage in one of the sites, the calculations would have been repeated under the assumption of two PNs. If a pair of PNs was still insufficient, the number would continually be incremented until there were enough port networks to handle the TDM usage in that particular site. Finally, the TDM resources on the two G350 Media Gateways are easily sufficient for supporting the 17.9 Erlangs of TDM traffic in Site 3.

Note:

The more PNs, the more inter-Port Network calls there are, and hence more TDM usage, since each interport network call requires resources in *each* PN that is involved in each call.

Next, the media processing resources must be considered. Since there are some fundamental differences between the TN2302AP and the TN2602AP media processors, they will be discussed separately, beginning with the TN2302AP.

Each TN2302AP IP Media Processor circuit pack (or Media Gateway VoIP Media Module) can support only a finite number of simultaneous calls. However, the exact number that can be supported varies according to the codecs of the calls to be supported. In general, compressed calls (for example, G.729 codec) require twice as many media processing resources as uncompressed calls (for example, G.711 codec). Also, calls utilizing AES media encryption require approximately 25% more media processing resources than unencrypted calls.

A TN2302AP circuit pack (or a MG VoIP Media Module) can support both compressed and uncompressed calls, as well as both encrypted and unencrypted calls, all simultaneously. Therefore, the general model for sizing the media processing resources is very complex. The model is a “batch arrival and service” model, and the details are beyond the scope of this document.

In practice, a fairly common strategy is to use an uncompressed codec for intrasite calls, and a compressed codec for intersite calls. This is due to the trade-off between bandwidth savings, increased media processing costs, and voice quality for compressed calls. If a private LAN is used for intrasite calls, bandwidth usage is of less concern than media processing cost and voice quality. However, for intersite calls, especially over a public WAN, the bandwidth savings offered by the use of compression outweighs the extra processing costs and slight degradation of voice quality.

Recall that any usage that is expressed in Erlangs represents the average number of busy servers at any given time. For the total media processing usages provided at the bottom of Table 34, a “server” can be thought of as the set of media processing resources that is necessary to support a single bidirectional media stream through a media processing circuit pack. Consider the total of 89.4 Erlangs of media processing usage in Site 1. This usage consists of 76.8 Erlangs of intrasite usage, and 12.6 Erlangs of intersite usage. Assume that an uncompressed codec is used for the intrasite calls, and a compressed codec is used for the intersite calls. Since each compressed call requires twice as many media processing resources as each uncompressed call, the 12.6 Erlangs must be counted twice. Therefore, the media processing load is actually 76.8 + (2 x 12.6) = 102.0 Erlangs. Similarly, the total media

processing loads in Sites 2 and 3 are 43.9 Erlangs and 17.6 Erlangs, respectively. Those numbers are also based on the assumption that media encryption was not used.

Table 35: Number of TN2302AP IP Media Processors or G700 Media Gateway VoIP Modules required for a given carried load

Carried load (Erlangs)	Required number of TN2302AP circuit packs	Carried load (Erlangs)	Required number of TN2302AP circuit packs
43	1	634	11
98	2	695	12
155	3	756	13
213	4	817	14
272	5	879	15
332	6	940	16
392	7	1,001	17
452	8	1,063	18
512	9	1,125	19
573	10	1,187	20

Table 36: Number of G350 Media Gateway VoIP Modules required for a given carried load

Carried load (Erlangs)	Required number of G700 MGs	Carried load (Erlangs)	Required number of G700 MGs
18	1	155	6
43	2	184	7
70	3	213	8
98	4	243	9
126	5	272	10

Table 35 implies that three TN2302AP IP Media Processor circuit packs should be used in Site 1 (Atlanta), and two should be used in Site 2 (Boston). Table 36 implies that the media processing resources on the two G350 Media Gateways in Site 3 (Cleveland) are easily sufficient. The required number of port networks, MGs, and media processing resources for Example 5: TDM and media processing usage is summarized in Table 37: TDM and Media Processing Requirements for Example 5: TDM and media processing usage on page 210.

Table 37: TDM and Media Processing Requirements for Example 5: TDM and media processing usage

Site	TDM Requirement	Media Processing Requirement
1	1 PN	3 TN2302AP boards
2	1 PN	2 TN2302AP boards
3	The 2 G350 MGs are sufficient	The on-board VoIP resources on the 2 G350 MGs are sufficient

TN2602AP IP Media Resource 320 differs from TN2302AP IP Media Processor both in capacity and regarding the degree of sensitivity to compression and encryption. While the capacity of a TN2302AP board is 64 simultaneous bidirectional, uncompressed, unencrypted connections, a TN2602AP board can be administered to support either up to 80 or up to 320 simultaneous bidirectional, uncompressed, unencrypted connections. Furthermore, while the capacity of a TN2302AP board is decreased when compression and/or encryption is used, the capacity of a TN2602AP board is not. Table 38 summarizes the media processing capacities of the TN2302AP and TN2602AP circuit packs.

Table 38: Maximum number of simultaneous media processor connections

Connection Type		Supported by					
		Single G250 Mother board	Single G350 Mother board	Single G700 Motherboard (DAF-1), or a Single Extra VoIP card for G700 (MM760)	Single TN2302AP Board	Single TN2602AP with Maximum Licensed Capacity of 80	Single TN2602AP with Maximum Licensed Capacity of 320
Un-encrypted	G.711	10	32[1]	64	64	80	320
	G.729	10	16	32	32	80	320
	G.723	10	16	32	32	NA	NA
	G.726	10	16	32	NA	80	320

1 of 2

Table 38: Maximum number of simultaneous media processor connections (continued)

Connection Type		Supported by					
		Single G250 Mother board	Single G350 Mother board	Single G700 Motherboard (DAF-1), or a Single Extra VoIP card for G700 (MM760)	Single TN2302AP Board	Single TN2602AP with Maximum Licensed Capacity of 80	Single TN2602AP with Maximum Licensed Capacity of 320
Encrypted	G.711	10	24	48	48	80	320
	G.729	10	12	24	24	80	320
	G.723	10	12	24	24	NA	NA
	G.726	10	12	24	NA	80	320
T.38 Fax or Modem over IP		10	8	16	16	80	320

1. 16 when transcoding G.711 to another codec.

Starting with release 3.1 of Communication Manager, the TN2602AP IP Media Resource 320 can be duplicated to provide critical bearer reliability for IP-connected port networks.

If more than one PN had been required in a particular site, intrasite calls between circuit-switched endpoints in that site would have contributed toward media processing usage because inter-Port Network calls between circuit-switched endpoints traverse an IP network. Since only one PN is required in each site in this example, the media-processing usage for calls between circuit-switched endpoints is zero in each site, as indicated in Table 34.

Processing occupancy

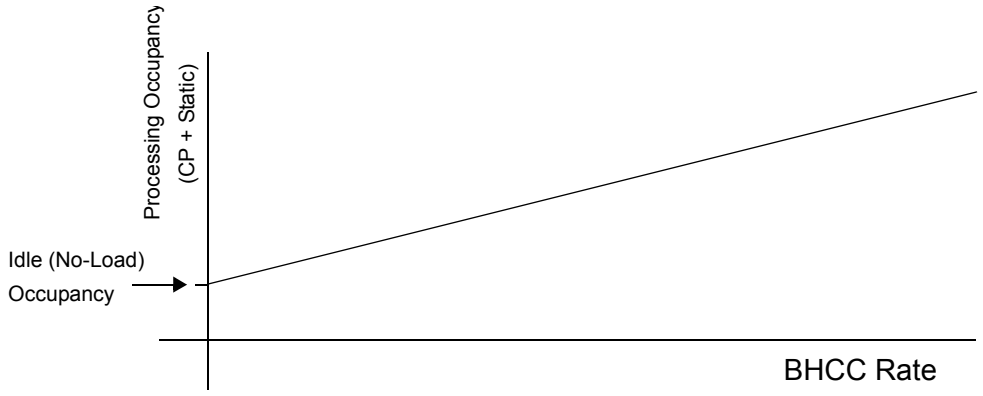
The Busy Hour Call Attempt (BHCA) rate of a system is the total number of calls that are attempted within that system, during its busy hour. This is distinct from the Busy Hour Call Completion (BHCC) rate of a system, which counts only those calls that have actually been completed. The *call capacity* of a system refers to its BHCC rate.

In Communication Manager products, server occupancy (or processor occupancy, as applicable) can be broken down into three categories: static occupancy, Call Processing (CP) occupancy, and system management (SM) occupancy. The static component refers to keep-alive processes, the CP component refers to processes that are required to set up and tear down calls (as well as vectoring operations, in the case of call centers), and the SM component refers to background maintenance operations and system audits. In theory, static occupancy is a fixed overhead, and CP occupancy is directly proportional to the call rate. SM

occupancy is allocated on an as-needed basis, such as for periodic maintenance functions. However, if the overall server occupancy exceeds a particular threshold, SM operations are postponed until a quieter traffic period.

Usually, the relationship between the sum of static and CP occupancy, as a function of BHCC, is linear, with a positive y-intercept, as illustrated in Figure 69: Relationship Between Processing Occupancy and BHCC Rate on page 212. The slope of the line corresponds to the average processing cost per call, and the intercept corresponds to the idle (that is, no-load) occupancy. The average processing cost per call depends on the mix of calls that is being handled by the system, and how complex each type of call is. For general business calls, nearly all of the CP occupancy is associated with setting up and tearing down calls. The call processing that is required for maintaining the call once it has been established is negligible in comparison, regardless of how long the call lasts. In a call center, the additional cost of processing vectoring steps throughout the lifetime of a call must also be considered.

Figure 69: Relationship Between Processing Occupancy and BHCC Rate



To determine the anticipated processor occupancy that is associated with a particular configuration, the average processing cost per call must be determined based on the anticipated volume of each type of call, and the complexity of the various call types. This average cost per call implies the slope of the line in relating static and CP occupancy to the BHCC rate. The intercept of that line, which corresponds to the no-load occupancy, depends on several factors, including which Communication Manager platform is being used, how many endpoints are administered, and so on.

Communication Manager systems are designed to keep the sum of static and CP occupancy below a particular threshold. This is done to allow a suitable amount of processing time for system management functions.

So for a given configuration, the various types of calls to be supported are identified, and the processing cost for each call type (based upon the complexity of the call) must be assessed. That information can then be used to determine the average processing cost per call, based on the anticipated relative frequencies of the various call types. The slope of the line relating the sum of static and CP occupancy can then be determined from the average processing cost per call. The intercept of that line is determined by information such as the Communication Manager platform used, the number of endpoints administered, and so on.

Therefore, for the given configuration, the specific linear model for the relationship between the sum of static and CP occupancy, as a function of BHCC, has been derived. Using the anticipated BHCC rate in that model yields the expected combined static and CP occupancy. If that value exceeds the preset threshold, the configuration is unacceptable for the anticipated call rate. In such a case, to support that call rate, either another platform must be considered, or multiple platforms must be networked together.

SIP traffic engineering

Traffic engineering and resource sizing for SIP involve several unique considerations:

- Direct media shuffling between SIP and H.323 endpoints
- SIP trunk provisioning and allocation
- SIP message traffic and its effect on message handling components
- Non-call related SIP traffic:
  - Registration
  - Subscription
  - Instant messaging
- Special configurations:
  - Bridging
  - Conferencing
- SES processor occupancy
- Communication Manager processor occupancy

Direct media connect (shuffling)

SIP phones shuffle to "direct media connect" with other SIP phones, but not with H.323 IP phones for releases up to Communication Manager 3.1. On systems with mostly SIP phones and few IP phones, or vice versa, the VoIP media resource traffic engineering is essentially similar to that of a system with only IP phones. Systems with significant numbers of both SIP and H.323 IP phones will need additional media processing resources to handle the added load from SIP-to-IP connections that do not shuffle.

Traffic engineering analysis starts with adding another separate type of endpoint, S (for SIP), to the expanded COI matrix discussed previously. Media connections between endpoints S and circuit-switched phones and trunks take up the same media processing resources as a call between IP phones and circuit-switched points. Connections between S endpoints and IP phones, however, take up media processing channels on both legs of a call.

Communication Manager release 4.0 and later supports direct media shuffling between SIP and IP stations, provided both endpoints support compatible codec and encryption options, as

usual. Direct media shuffling between SIP stations and IP trunks is not supported. Therefore, SIP calling between Communication Manager systems connected by IP TIE trunks always require allocation of VoIP media resources.

C-LAN allocation and SIP trunks

The Communication Manager server communicates to the SES server over administered SIP trunks, which are finite software entities similar to H.323 IP TIE trunks. Communication Manager organizes SIP trunks into trunk groups just like other trunks of any type. Each SIP trunk group signals through a C-LAN or PC-LAN socket as a single signaling group. A SIP trunk group may contain up to 255 trunk members.

Each leg of a SIP call in progress takes up one SIP trunk member for the duration of the call. Thus, a SIP-SIP call takes up two trunk members, although those trunk members corresponding to the two SIP endpoints need not be in the same trunk group, C-LAN, or SES. Provisioning SIP trunks is then a process similar to provisioning IP and PSTN trunks, a matter of accounting for traffic load and application of the standard Erlang calculations outlined in previous sections. Calls routing to (terminating at) SIP endpoints can go through any C-LANs with SIP trunks administered to the endpoint's home SES. But calls originated by a SIP endpoint can only route to a specific C-LAN according to the administered routing table in the home SES; if all trunk members on that C-LAN are in use, the SIP endpoint-originated call is blocked. Therefore, the prudent but somewhat conservative way to allocate SIP trunks is to treat each C-LAN as a distinct trunk resource for both SIP endpoint-originated and endpoint-terminated calls. In other words, allocate enough trunk members on each C-LAN to achieve the desired grade of service within each C-LAN, not treating all trunk members in all C-LANs as a pool.

Systems that use C-LANs to provide the signaling sockets for SIP trunks require additional traffic engineering. Each C-LAN and IPSI circuit pack has finite processing capacity, which translates into a finite message handling throughput. Each SIP call, just like an H.323 or an H.248 call, involves some amount of upstream (endpoint to server) and downstream (server to endpoint) message traffic through intermediate components like C-LAN and IPSI. Therefore, finite message throughput for IPSI and C-LAN means finite call volume signaled through those components. Being a text based protocol, SIP signaling involves much larger messages compared to binary protocols. Generally, each C-LAN can handle signaling for 4000 to 10,000 SIP calls per hour (a call between two SIP phones signaled through the same C-LAN counts as two calls), depending on the complexity of the call. IPSI has 3 to 4 times the signaling throughput capacity of C-LAN.

Combining both traffic considerations of trunk member allocation and signaling throughput, C-LAN provisioning is thus an iterative process:

1. Allocate an initial guessed number of C-LANs.

   Quick rule: 1000 to 4000 users per C-LAN, depending on assumed complexity of each SIP call (more complex implies fewer users per C-LAN).

2. Assign SIP endpoints to C-LANs.

   Can uniformly distribute or allocate according to user community, if such information exists.

3. Allocate enough trunk members to each C-LAN to achieve desired grade of service, based on the known or assumed call traffic.
4. Check SIP message throughput based on the call traffic.
5. If SIP message traffic exceeds desirable threshold for any C-LAN, either add more C-LANs or re-distribute users, if excess capacity exists in any C-LAN.

   Return to Step 2. Otherwise, continue to Step 6.
6. Assign C-LANs to port networks and IPSIs.

   Estimate IPSI loading; add more PN and IPSI, if necessary.

SIP specific features

SIP deals with much more than just traditional voice communication. Any traffic analysis must incorporate considerations of the following essential SIP features:

Registration

When large numbers of endpoints start up nearly simultaneously, the system must handle the resulting flood of registration traffic in a robust and timely manner. The requirements and issues are similar to the case for H.323 endpoints, except that SIP deals with two servers: SES and the Communication Manager server.

Subscription and notification

Endpoint subscriptions to events, such as presence, features, message indicator, and bridges, can potentially generate a large signaling load from the resulting notification message traffic. Consider that, if each SIP user has average of "S" subscriptions (other users) subscribing to its presence, then "U" users averaging "P" presence changes (off-hook, on-hook, unavailable, etc.) per hour generates "S x U x P" notifications per hour.

Instant messaging

The Avaya SIP SoftPhone supports instant messaging (IM) over SIP. Experience and data on average usage patterns for IM (average session time, message size, frequency, etc.) is currently somewhat sparse. This could be a minor part of SIP traffic, at least for near future deployments. But judging by the proliferation and popularity of IM among the consumer public, its future potential cannot be discounted.

These are just some of the SIP features not considered in the traditional call traffic models. Given that SIP is a constantly evolving and expanding standard, more non-call related SIP traffic can be expected in the future. Some traffic, such as registration and subscription/ notification, involve both the SES and Communication Manager servers, and thus affect load on such message bearing components as C-LAN and IPSI. Others, such as IM, will only affect SES. Therefore, a SIP traffic model must account for the various types of traffic, their respective flow patterns, and resulting loads on components.

Communication Manager and SES server processor occupancy

SIP incurs Communication Manager server processing time (as discussed in a previous section), just like any other type of Communication Manager call. Special care should go into accounting for the SIP features present in an average call. Calls involving notifications because of bridging or subscriptions can be significantly more CPU intensive than simple calls.

Since SES is an integral part of all SIP calls, its CPU resource requires proper accounting just like Communication Manager servers. Additionally, SES is more than just a SIP proxy, routing a SIP message, it is an all-in-one solution housing multiple additional servers and functions defined in the SIP standard: presence, event, personal profile, etc. Therefore, the SES is much more involved than the Communication Manager server in the processing of SIP messages, especially those outside of traditional call setup and teardown. A comprehensive traffic model for SES must account for both call and non-call related traffic load.

IP bandwidth and Call Admission Control

IP bandwidth analysis for media streams begins with determining the number of bidirectional media streams that are associated with each type of call supported by the system. Throughout this discussion, calls between two IP stations are assumed to use shuffling. That being the case, Figure 66: Connectivity modes between two IP endpoints on page 202 indicates that an intrasite call between two IP endpoints requires a single bidirectional media stream through the LAN at that site. Figure 65: Examples of media streams between Avaya endpoints on page 200 indicates that each intrasite call between an IP endpoint and a circuit-switched endpoint (including PSTN trunks) also requires a single bidirectional media stream through the LAN at that site. In addition, Figure 65: Examples of media streams between Avaya endpoints on page 200 indicates that each interport network intrasite call between two circuit-switched endpoints (including PSTN trunks) also requires a single bidirectional media stream through the LAN at that site (assuming that IP-PNC is used, as opposed to a circuit-switched center stage). In fact, the only intrasite call that does not require a single bidirectional media stream through the LAN at that site is an intraport network call between two circuit-switched endpoints which requires no IP resources because the call is completed solely across the circuit-switched TDM bus of the PN. Each intersite call requires exactly one bidirectional media stream through each participating site's LAN, as well as a single bidirectional media stream through the WAN that connects the two sites.

The preceding discussion is summarized in Figure 70: Required number of bidirectional IP media streams for intra-site calls on page 217 and Figure 71: Required number of bidirectional IP media streams for inter-site calls on page 217.

Figure 70 and Figure 71 provide information about the required number of bidirectional media streams per call. This information can be combined with call usage information to provide IP bandwidth usage estimates, as shown in Example 6: IP bandwidth considerations.

Figure 70: Required number of bidirectional IP media streams for intra-site calls

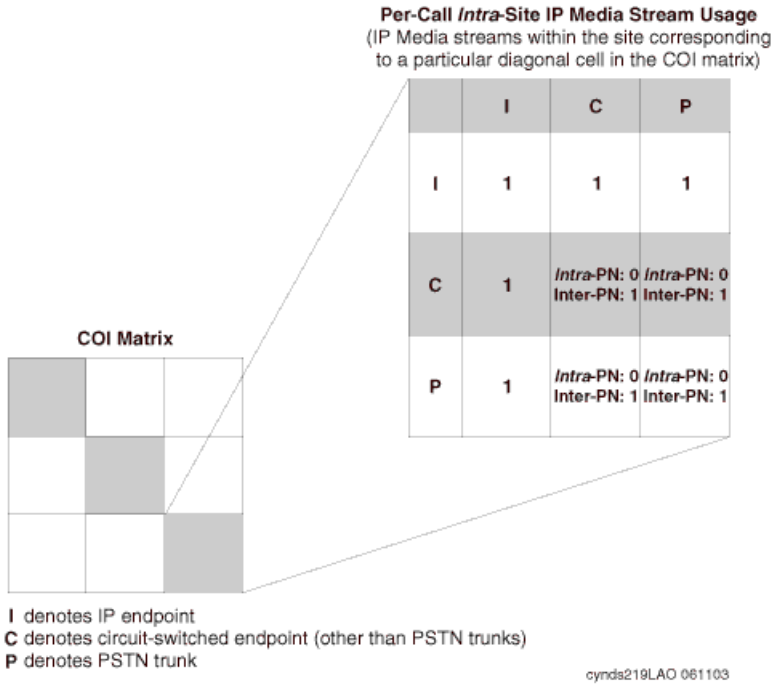
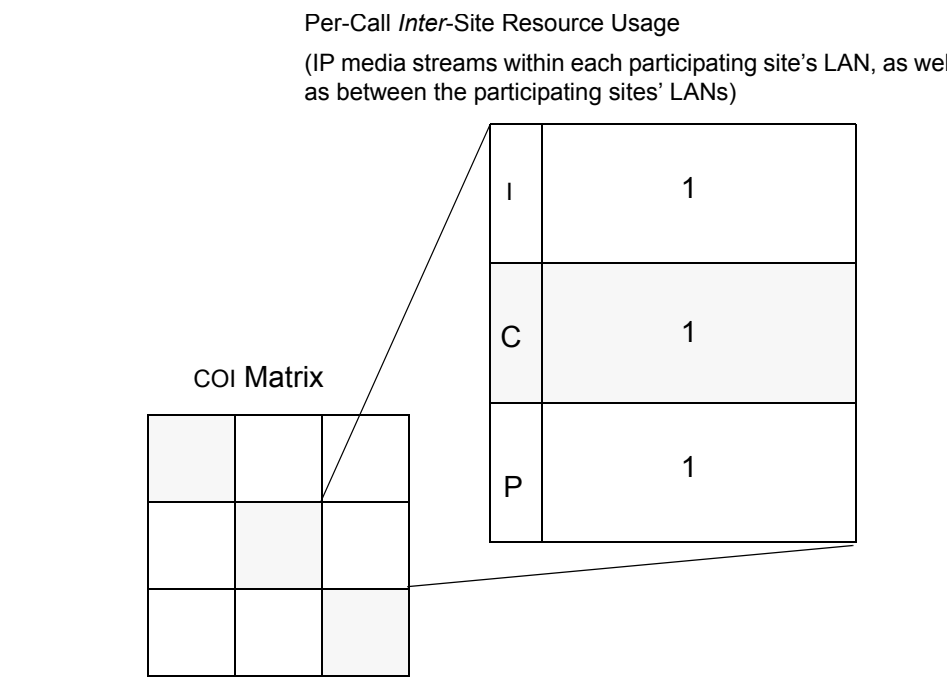


Figure 71: Required number of bidirectional IP media streams for inter-site calls



Example 6: IP bandwidth considerations

The information in Figure 70 and Figure 71 along with the information in Table 33 produces the following tables of bandwidth usages that are associated with the configuration in Example 4: Expanded COI matrices.

Table 39: IP LAN bandwidth usages (Erlangs) for Example 6: IP bandwidth considerations

Endpoints	Site 1 (Atlanta)	Site 2 (Boston)	Site 3 (Cleveland)
Intrasite: I, I	12.7	1.9	0.78
Intrasite: I, C or P	76.8	26.7	14.4
Intrasite: C or P, C or P	0	0	0
Calls from site 1 to site 2	12.0	12.0	0
Calls from site 2 to site 1	12.0	12.0	0
Calls from site 1 to site 3	5.0	0	5.0
Calls from site 3 to site 1	5.0	0	5.0
Calls from site 2 to site 3	0	2.0	2.0
Calls from site 3 to site 2	0	2.0	2.0
Totals	123.5	56.6	29.2

Table 40: IP WAN bandwidth usages (Erlangs) for Example 6: IP bandwidth considerations

Endpoints	WAN bandwidth (Erlangs) between Sites 1 and 2	WAN bandwidth (Erlangs) between Sites 1 and 3	WAN bandwidth (Erlangs) between Sites 2 and 3
Calls from site 1 to site 2	12.0	0	0
Calls from site 2 to site 1	12.0	0	0
Calls from site 1 to site 3	0	5.0	0
Calls from site 3 to site 1	0	5.0	0

1 of 2

Table 40: IP WAN bandwidth usages (Erlangs) for Example 6: IP bandwidth considerations (continued)

Endpoints	WAN bandwidth (Erlangs) between Sites 1 and 2	WAN bandwidth (Erlangs) between Sites 1 and 3	WAN bandwidth (Erlangs) between Sites 2 and 3
Calls from site 2 to site 3	0	0	2.0
Calls from site 3 to site 2	0	0	2.0
Totals	24.0	10.0	4.0

2 of 2

Table 39 and Table 40 express bandwidth usages in Erlangs, because each such usage actually represents the average number of simultaneous bidirectional media streams through the IP network in question. To convert those usages into bandwidth requirements in units of kilobits per second (kbps), one must know how many kbps each call requires. To answer that question, a closer look at IP packet structure is necessary.

An IP packet consists of a payload and some amount of overhead. The payload consists of actual sampled voice, and the overhead represents headers and trailers, which serve to navigate the packet to its proper destination. The overhead due to IP, UDP, and RTP is 40 bytes, while the Ethernet overhead is between 18 and 22 bytes (18 is assumed in this example). This represents a total overhead of 58 bytes (464 bits), regardless of the nature of the payload. For this example, Layer 2 (Ethernet) overhead is included in that total. At every router boundary, because Ethernet overhead is included in this example, our calculations are for bandwidth on a LAN. Because WAN protocol (for example, PPP) Layer 2 headers are generally smaller than Ethernet headers, WAN bandwidth is slightly less than LAN bandwidth.

The size of the payload depends on certain parameters that relate to the codec that is used. The two most common codecs that are used with Avaya products are uncompressed G.711 and compressed G.729. The transmission rates that are associated with those codecs are 64 kbps for G.711 (this is the Nyquist sampling rate for human voice) and 8 kbps for G.729.

The packet “size” is sometimes expressed in units of time (specifically, in milliseconds). The following formula yields the packet size, expressed in bits:

$$\text{Number of bits of payload per packet} = \left(\text{Transmission Rate (kbps)}\right) \times (\text{ms per Packet})$$

Table 41: Payload size per packet on page 220 is populated using this formula, and provides the payload size per packet (expressed in bits) as a function of packet "size" (that is, ms per packet) and codec.

Table 41: Payload size per packet

Packet "size" (ms)	G.711 (bits)	G.729 (bits)
10	640	80
20	1280	160
30	1920	240
60	3840	480

Note that the number of bits of payload per packet depends on the packet "size," but it is independent of the "sizes" of the individual frames that are contained in that packet. For example, a packet "size" of 60 ms could be referring to six 10-ms frames per packet, or three 20-ms frames per packet, or two 30-ms frames per packet, and so on. Presently, the most commonly used packet "sizes" are 20 ms. Both G.711 and G.729 codecs typically use two 10-ms frames per packet.

As stated earlier, there is an overhead of 464 bits per packet. So, the bandwidth (expressed in kbps) that is associated with a unidirectional media stream (assuming no Silence Suppression is used) is augmented from 64 kbps and 8 kbps (for G.711 and G.729, respectively) to account for this overhead. The results of this exercise are provided in Table 42: Bandwidth requirements for media streams.

Table 42: Bandwidth requirements for media streams

Packet "size" (ms)	G.711 (kbps)	G.729 (kbps)
10	110.4	54.4
20	87.2	31.2
30	79.5	23.5
60	71.7	15.7

Note that the entries in Table 42 correspond with a single (unidirectional) media stream. As we will see in the following example, the entries in Table 42 are not multiplied by the *average* number of simultaneous streams, but rather by a much larger number that represents the 99.9th percentile for the simultaneous number of streams.

Example 7: LAN bandwidth

In Example 6: IP bandwidth considerations, the total IP LAN bandwidth usage for each site was calculated, and expressed in Erlangs at the bottom of Table 39. Specifically, the total LAN bandwidth usage in Site 1 is 123.5 Erlangs, in Site 2 is 56.6 Erlangs, and in Site 3 is 29.2 Erlangs. This implies that the average number of bidirectional media streams that are simultaneously in use at any given time in Site 1 is 123.5. Analogous statements can also be made regarding Sites 2 and 3.

Every media stream across the IP LAN in any of the three sites is assumed to use the uncompressed G.711 codec, since bandwidth is relatively inexpensive within a private LAN, as opposed to a public WAN. Assume, for the sake of this example, a standard IP packet size of 20 ms. So for the G.711 codec, Table 42 indicates that each media stream consumes 87.2 kbps of IP LAN bandwidth. It may be tempting at this point to simply multiply 87.2 kbps by 123.5 simultaneous bidirectional media streams, to arrive at the estimate for the overall LAN bandwidth needed for Site 1. However, 123.5 is merely the *average* number of simultaneous media streams, and approximately half of the time, there are at least 124 simultaneous media streams in use.

In this example, suppose that the goal is to supply enough bandwidth to adequately support the media streams at least 99.9% of the time. The standard infinite-server queueing model implies that less than 0.1% of the time there are at least 159 simultaneous media streams in the Site 1 LAN. So, it is sufficient to engineer the LAN bandwidth to support 158 simultaneous media streams. Therefore, the Site 1 LAN requires at least (158 simultaneous media streams) x (87.2 kbps per media stream) = 13.8 Mbps of bandwidth, in each direction. This result, along with the analogous results for Sites 2 and 3, are provided in Table 43: IP LAN bandwidth requirements in each direction, for Example 7: LAN bandwidth.

Table 43: IP LAN bandwidth requirements in each direction, for Example 7: LAN bandwidth

Resource	Site 1 (Atlanta)	Site 2 (Boston)	Site 3 (Cleveland)
Simultaneous media streams for “P001”	158	81	47
LAN bandwidth (Mbps)	13.8	7.1	4.1

In Table 43, the number of simultaneous media streams for “P001” represents the 99.9th percentile for the number of simultaneous unidirectional streams, as determined by applying the standard infinite-server queueing model.

A slight variation of the procedure that was used to determine LAN bandwidth in Example 7: LAN bandwidth can be used to determine WAN bandwidth. Using compressed RTP (cRTP) is a means to conserve bandwidth. Specifically, the use of cRTP reduces the overhead due to IP, UDP, and RTP from 40 bytes to between 2 and 4 bytes (4 bytes are assumed for this example). Using the PPP overhead of 7 bytes (which would vary if ATM, HDLC, or Frame Relay were used) implies a total overhead of 11 bytes (88 bits) in this example. This implies the following

table of WAN bandwidths, Table 44: IP WAN bandwidth requirements for media streams on page 222, which assumes the use of cRTP:

Table 44: IP WAN bandwidth requirements for media streams

Packet "size" (ms)	G.711 (kbps)	G.729 (kbps)
10	72.8	16.8
20	68.4	12.4
30	66.9	10.9
60	65.5	9.5

This table can be used in the WAN bandwidth calculation for the system in Example 6: IP bandwidth considerations.

Example 8: WAN bandwidth

In Example 6: IP bandwidth considerations, the total IP WAN bandwidth usage between each pair of sites was calculated, and expressed in Erlangs at the bottom of Table 40. Specifically, the total WAN bandwidth usage between Sites 1 and 2 is 24.0 Erlangs, between Sites 1 and 3 is 10.0 Erlangs, and between Sites 2 and 3 is 4.0 Erlangs. This implies that the average number of media streams simultaneously in use at any given time between Sites 1 and 2 is 24. Analogous statements can also be made regarding WAN traffic between each of the other two pairs of sites.

Every media stream across the IP WAN, between any pair of sites, is assumed to use the compressed G.729 codec, since bandwidth is relatively inexpensive within a private LAN, as opposed to a public WAN. Assume, for the sake of this example, a standard IP packet size of 20 ms. For the G.729 codec, Table 44 indicates that each (unidirectional) media stream consumes 12.4 kbps of IP WAN bandwidth. Similar to the case in Example 7: LAN bandwidth, 24 is the *average* number of simultaneous bidirectional media streams. As in Example 7: LAN bandwidth, the bandwidth is sized to a "GOS" of P001 ("GOS" in this context is actually a pseudo-GOS; true GOS is associated with a fixed number of channels, as is typical of circuit-switched systems). The standard infinite-server queueing model implies that less than 0.1% of the time there is at least 40 simultaneous media streams between Sites 1 and 2. So, it is sufficient to engineer the WAN bandwidth between those two sites to support 39 simultaneous media streams. Therefore, the WAN between Sites 1 and 2 requires at least (39 simultaneous media streams) x (12.4 kbps per media stream) = 484 kbps of bandwidth. This result, along with the analogous results for the WAN traffic between the other two pairs of sites, are provided in Table 45: IP WAN bandwidth requirements in each direction, for Example 8: WAN bandwidth on page 223.

Table 45: IP WAN bandwidth requirements in each direction, for Example 8: WAN bandwidth

Requirement	Between sites 1 and 2	Between sites 1 and 3	Between sites 2 and 3
Simultaneous media streams for “P001”	39	20	10
LAN bandwidth (kbps)	484	248	124

In Table 45, the number of simultaneous media streams for “P001” represents the 99.9th percentile for the number of simultaneous streams, as determined by applying the standard infinite-server queueing model.

To this point, all the discussion regarding bandwidth relates only to bearer traffic (media streams). Network packet traffic that is related to signaling is very different from the bearer traffic because it tends to occur in bursts. For example, while the bearer traffic that is associated with a particular call tends to involve a constant, steady stream of packets throughout the duration of that call, the signaling traffic for that same call tends to occur in bursts during call setup and teardown.

The bandwidth that is required for signaling is generally negligible in comparison to the bandwidth that is required for bearer traffic. However, since Avaya products use Separation of Bearer and Signaling (SBS), the bearer traffic and signaling traffic use distinct paths. Therefore, signaling bandwidth must be given its due consideration, despite the fact that it is negligible in comparison to bearer bandwidth.

Signaling traffic is more prone to bursts than bearer traffic because the former consists of messages that are associated with call set-ups and tear-downs, as opposed to traffic that is uniformly distributed throughout entire call durations. However, the “burst” effect is somewhat assuaged for larger call volumes. Although the precise bandwidth requirement for a given configuration depends on the nature of the endpoints involved, a reasonable approach is to allocate an overhead of 50 bits per second (bps) for each IP endpoint in the network, as well as the following (as applicable) for every 1000 calls:

- 11 kbps for messaging between the S8700-series Server and an IPSI circuit pack on a G650 Media Gateway
- 8 kbps for the H.248 link between a C-LAN circuit pack and a G700 or G350 Media Gateway

Note:

The 11 kbps and 8 kbps associated with 1000 calls should not be amortized to produce estimates for systems with very light traffic. For example, 11 bits per second and 8 bits per second will not support an individual call.

Physical resource placement

As a default, resources should be balanced as uniformly as possible. For example, if 11 Media Processors are required in a Network Region that has three PNs, two of the PNs should house four Media Processors each, and the other PN should house the final three Media Processors. This applies to signaling components C-LANs and IPSIs, also. The MGs usually generate much more signaling traffic than IP endpoints, even though they each take up one only socket on the C-LAN and one DLCI on the IPSI. Therefore it is advisable to practice even distribution for both MGs and IP endpoints among available C-LANs, IPSIs, and the port networks they reside in. Advanced users should be able to manually override the resource-placement defaults. For example, there might be reasons beyond traffic engineering for specifying an unbalanced system or an over-engineered resource pool, such as reliability, cost, security, physical constraints, and so on.

Final checks and adjustments

The final step in the design process is to verify that the final configuration proposal meets the following criteria:

- All endpoints and media gateways have been assigned to various Network Regions, sites, and/or Communication Manager systems, according to customer specifications.
- The placement of resources adheres to the physical capacities of the proposed platform.
- The number of PNs and/or Media Gateways is sufficient to handle the TDM traffic, the required number of IPSI circuit packs, and the required number of port circuit packs.
- The number of C-LAN circuit packs is sufficient to support the desired number of IP endpoints, Media Gateways, and certain adjuncts.
- The number of media processing circuit packs is sufficient to handle both calls involving IP endpoints, and interport network calls between circuit-switched endpoints, unless a circuit-switched center stage is used instead of IP-PNC.
- The anticipated call volume can be handled by the server.
- There is sufficient bandwidth in all IP networks to support the anticipated media traffic.

Avaya Distributed Office

Distributed Office is a communications system consisting of a number of geographically dispersed nodes or branches. Each branch contains a Distributed Office branch solution running both a SIP proxy server and a SIP feature server for local endpoints. The single-location Distributed Office solution makes up a self-contained communication system capable of providing services to local phones and trunks. Distributed Office branch locations are managed by the Distributed Office Centralized Management, a tool running from a single location, and by Distributed Office Local Manager, individualized management at each location. For smaller deployments or for a stand-alone branch, the Local Manager may suffice. Central and Local Management may be used together in a synchronized manner to provide complete administration and maintenance for Distributed Office.

Distributed Office has two branch hardware platforms: the i40, based on the various G250 gateways supporting up to 40 stations per branch, and the i120, based on the G350 gateway supporting up to 120 stations per branch. The i40 and the i120 generally observe the same resource configuration rules and constraints — for example, for VoIP channels, touch tone detectors, announcements ports, available media modules slots — as the G250 and G350 gateways on which they are based. Therefore, traffic engineering for each Distributed Office branch includes the same considerations as those for the corresponding G250 and G350 gateways.

Using SIP, the SES edge router mediates all communication between branch locations. An SES edge can support up to 1000 Distributed Office branches averaging up to 40 users per branch, for a total of up to 40,000 stations. The SES edge also handles traffic within one or more main sites consisting of one or two regular SES homes servicing one or two Communication Manager systems.

SIP traffic through the SES edge consists of the follow flows:

1. Branch-to-branch call traffic
2. Branch-to/from-main site(s) call traffic

   Note:

   A main site consists of a large headquarters or business location served by Communication Manager systems and SES homes.
3. Main site(s) call traffic between Communication Manager systems not linked by non-SIP TIE trunks
4. Instant messaging between branches and SES homes
5. Presence subscription notification traffic between branches and SES homes

Traffic engineering for the SES edge consists of tracking and estimating the SIP message routing through the SES edge based on the above message flows. Since there can be only one SES edge, there is nothing to "configure," per se. Instead, traffic engineering provides an estimate of the traffic volume handled by the SES edge and compares it to known hardware performance levels to ensure a robust functioning system operating well-under projected limits.

Of the flow components listed above, the first three, related to call traffic, should be the most commonly considered loads. Call traffic patterns and profiles heavily depend on the specific type of business conducted at the branches, such as retail, support, marketing, insurance, real estate. However, we generally expect a large portion of the branch call traffic to be confined to the branch — that is, call signaling handled entirely within the branch without routing through SES edge. These intra-branch calls include local PSTN calls at the branch location over analog, BRI, or T1 connections to the local central office. Only a smaller fraction (10-20%) should route outside the branch through the SES edge. This is why a single SES edge server can support 1000 branches and 40,000 stations.

Instant messaging and presence subscriptions are relatively new forms of traffic load and their use depends on user adoption. Therefore, traffic loads for these services are currently difficult to predict. Presence subscription, in particular, scales as the product of presence users and subscribers, and has potential to scale as the square of the user population, quickly becoming the dominant load.

Avaya has developed detailed traffic flow models to estimate the load on an SES edge based on the analysis described above. With these tools, we can ensure proper deployments based on individual customer needs.

Security

This chapter discusses the security design and features for Avaya Communication Manager, and how to operate Avaya systems securely.

Note:

Because this information is valuable both to those who want to protect the system and to those who seek to “hack” into those systems, the information in this section is deliberately incomplete. For example, we discuss the use of one-time passwords for user authentication, but not the mechanism of how this feature works.

Earlier systems did not interface with the data network and were neither susceptible to the types of attacks that are prevalent on those networks, nor provided a gateway into such networks from which an attack might be launched. With the convergence of voice (IP Telephony) and data over corporate enterprise networks, this is no longer true.

The main topics included in this chapter are:

- Your security policy
- Avaya Communication Manager and Servers
- IP Telephony circuit pack security
- Toll fraud

For additional information about IP Telephony security, see *Security Design and Implementation for Avaya Voice over IP*, 03-601973.

Your security policy

System security does not begin with the system itself, but with the people and the organizations that operate or use the system. One of the most important tools for securing a system is to have a written, published, and enforceable *security policy*. Your security policy should clearly address these questions:

- What are you trying to protect?
- What are you protecting it from?
- How likely is a threat against these assets?

What are you trying to protect?

The security policy usually attempts to protect information, whether the information is in the form of data (files) or conversations (digitized voice packets). Customers should assess the value of those assets that require protection, and compare the true costs of security to the value of those assets.

What are you protecting it from?

Most often, criminals, who are also called “hackers,” pose a significant threat to secure information. However, do not forget to look internally. A significant number of attacks come from within an enterprise. Your security policy should include rules about behavior, the consequences of bad behavior, a path of escalation, and a person to contact with regard to security issues.

How likely is a threat against these assets?

Security is always a trade-off. The more security, the more inconvenience and the more cost. To avoid the necessary inconvenience, some users are likely to subvert the security policy. For example, if you make passwords so complex so that the passwords are difficult to remember, people will write the passwords down. Users prefer easy access without security. Having to log on is inconvenient. However, everyone must endure some level of inconvenience if the system is going to be secure against attacks. The security policy must define this level of inconvenience to ensure that the security polity is not circumvented. In addition, management must support the policy, and establish clear rules for its enforcement, including the consequences for violating it. A security policy that does not establish consequences for violations quickly becomes irrelevant.

Recommendations for your security policy

Avaya recommends that you continuously review your security policy, and keep up with new threats and to make improvements each time a weakness is found. To effectively support your security policy, your company must allocate long-term resources to the development, implementation, and reassessment of the policy.

Avaya Communication Manager and Servers

This section discusses Avaya's security designs:

- Built-in Linux security features
- One-time passwords
- Shell access
- Root access
- Remote access
- Secure access
- Monitoring and alarming
- Data encryption

Built-in Linux security features

Proprietary vs. open operating systems

Open operating systems such as Linux or a version of Microsoft Windows are often thought to be less secure environments compared to proprietary systems. To some extent this is true, but it is important to understand why Oryx-Pecos, Avaya's proprietary operating system for its legacy products, is more secure than an open operating system because it does not support the types of network connections that converged voice and data network configurations demand. So why not enhance Oryx-Pecos? Aside from the economic reasons, there is a security paradox: to make an operating system secure, reveal its inner most secrets. When the operating system software is publicly available and implemented in varying environments for a wide range of applications, there are many more eyes looking for security holes. The expertise of the entire technical community is brought to bear on the problem. Of the major operating systems (Unix, Linux, Windows), one is not inherently more secure than another. Each has inherent security flaws. All can be made secure through the application of a good security policy, which includes proper administration and configuration, and diligent application of vendor updates when security problems are discovered.

The Linux environment has a security advantage because

- Problems can be identified both by testing (hacking) and by reviewing the source code itself.
- Security "holes" tend to be fixed more quickly compared to proprietary operating systems.

Avaya capitalizes on Linux' security advantage

The Avaya servers run under the Linux operating system that has two important security features:

- Built-in protection against certain types of Denial of Service (DOS) attack, such as SYN floods, ping floods, malformed packets, oversized packets, sequence number spoofing, ping/finger of death, etc. Attacks are recognized at the lower levels of the software and their effect is blunted. (It is not possible for a target system to always provide service during a DOS attack. Rather, the protection is to automatically resume service as soon as the attack is removed.)
- The Linux kernel is compiled with a set of options to precisely tailor its operation to maximize security consistent with required operation of the system. These include a number of built-in firewall and filtering options. All file and directory permissions are set to minimize access as much as possible consistent with proper system operation. The disk drives of the S8700-series, S8500, and the S8300 Servers contain multiple partitions, each of which is restricted according to the type of data that it contains. All unneeded services are disabled either permanently or through administration for those services. Disabled services and capabilities include NFS, SMB, X-windows, rcp, rlogin, and rexec. The system administrator has additional control of which services are visible from the multiple Ethernet interfaces that are connected to the enterprise LAN. Other Ethernet interfaces are permanently configured to restrict services.

One-time passwords

Standard login accounts use static passwords that can be used multiple times to log in to a system. Anyone who can monitor the login messages can also capture passwords, and use the passwords to gain access. You can administer the Avaya servers for one-time passwords that have a fixed-user name but not a fixed password. In this case, users must supply a unique, one-time password for each session, and even if the password is compromised, it cannot be reused. When a system is covered by an Avaya service contract, all logins that are accessed by Avaya Services technicians are protected by one-time passwords.

Shell access

Access to a "shell" from which arbitrary commands can be executed is not granted by default to a login on an Avaya server. When a login is created, the system administrator can specify whether or not the account is permitted to have shell access. Accounts that are denied shell access can either log in to an Avaya Communication Manager administration screen or a Web page upon successful login. In both cases, the operations that these logins can perform are restricted. Generally, only people who perform hardware maintenance or software maintenance on the server need shell access permissions administered in their login accounts.

Root access

On a Linux system, the highest administrative-access level is called *root*. Direct logins to root-level accounts are not permitted on Avaya servers. Administrative access, which requires root-level permissions, is handled through “proxy” programs that grant specific access to specific accounts. The ability to obtain full, root-level access is granted only in very special circumstances. By tightly restricting the root password, Avaya systems are less susceptible to accidental or malicious system access.

Remote access

Avaya servers have a modem port for remote maintenance access, and for sending maintenance alarms calls. The server logins that establish this remote connection are separate from other logins that allow administrative functions. One login account can establish a connection, and once the link is established, a second login is necessary to administer the system. The dial-in line can also be restricted to:

- Disallow all incoming calls.
- Allow only one incoming call.
- Allow all incoming calls.

When the interface is set to “allow one incoming call only,” the line is enabled to answer a single call. As soon as a call arrives, the line is disabled, and must be re-enabled through administration before another call will be accepted. This feature does not inhibit outgoing alarm calls, which are needed for maintenance. Normally, the line is disabled for all calls. When a maintenance activity is needed, the maintenance technician must contact the server administrator and request that the line be activated. The server administrator must then log in to the server, and enable the line for one call only. The maintenance technician then calls the server, performs the necessary maintenance, and disconnects. At this point the line is automatically disabled again. Enabling the data line for one call only is a good example of a feature that illustrates the trade-off that is required between security and convenience. Having the data line disabled provides better security, but during diagnostic activity, when multiple calls must be made, the server administrator must be called to manually re-enable the line for each call. In addition, Avaya employs Expert systems technology to contact systems automatically for monitoring and diagnostics. Disabling the data line disables this technology, which results in higher maintenance costs, and possibly longer times out of service when a failure does occur.

Secure access

Typical server access methods include telnet, Web browser (HTTP), and FTP for file transfers. Each of these mechanisms can support login authentication, but suffer a common weakness. The password that you type during login is sent in clear text, which allows someone with a network monitor/sniffer to capture the password and to gain access. These mechanisms also transmit all the session information in clear text. Some of this information might contain data such as account codes, authorization codes, or other data that might be useful to an attacker.

To overcome these problems, Avaya servers support:

- Secure Shell Access (SSH) and Secure Copy (SCP). Provide an access mechanism for terminal access and file copy that encrypt the entire session, including the login sequence, and subsequent data transfer. ***SCP is the preferred method of transferring files.***
- Secure WEB access using the Secure Sockets Layer (SSL) with HTTPS. All Web access to an Avaya S8700 and S8300 servers is through a secure connection. Unencrypted Web access is not supported. The Avaya servers also support one-time-passwords for logins through these mechanisms, even though the exchange is already encrypted.
- FTP service that is disabled by default. Each time a file is to be transferred to the Avaya server, an administrator must log in and enable the FTP server. The file is then transferred using anonymous FTP, and the FTP server can then be disabled. Using anonymous FTP in this manner avoids the problem of sending passwords in clear text.

Monitoring and alarming

Avaya servers support the following security monitoring and alarming features:

- Sessions are automatically disconnected after a period of inactivity.
- Accounts are automatically locked out for a period of time as a consequence of consecutive failed login attempts.
- Files and directories are monitored and audited by Tripwire, which maintains a cryptographically encoded signature of the files on the system, and generates alarms if any changes occur.
- All login sessions, whether successful or not, are logged.
- User activity logging.
- Security events are alarmable and reported by sending an SNMP trap to one or more destinations.

Data encryption

Attacks against a system are not limited to attempts to find holes in the access structure. Avaya servers store backup copies of critical configuration information, including authentication and account information, on external systems. If this information is stored in clear text, and the file server on which it is stored is compromised, the servers also can be compromised. S8700 and S8300 servers can encrypt all backup data, and thus make use of the data impossible, even if access to it is possible. The user is responsible for remembering the encryption key, because Avaya cannot assist you if you forget it. Avaya also cryptographically signs all new software or firmware media to prevent malicious modification in transit. If the system detects a modification, the installation is aborted.

LAN isolation configurations

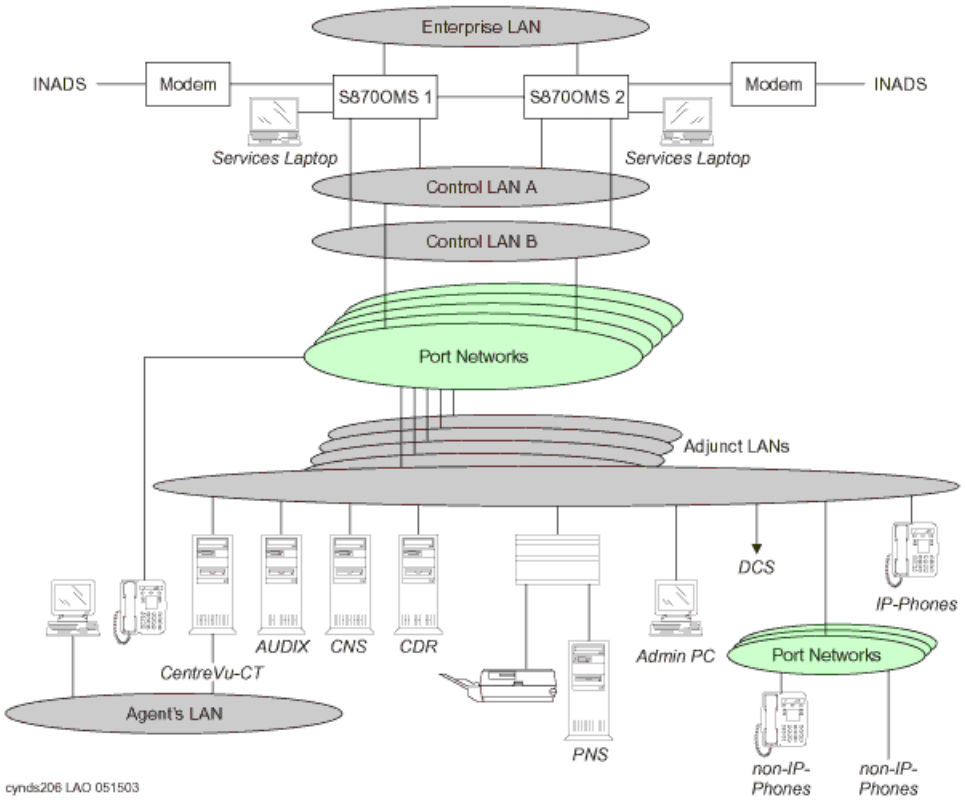
S8700 with Avaya MCC1 or SCC1 Media Gateways

An Avaya S8700-series Server contains multiple Ethernet Network Interfaces (NICs):

- Each Avaya S8700-series Server with Avaya MCC1 or SCC1 Media Gateway has five Ethernet interfaces (NICs), each dedicated to these specific functions:
  - The two control LANs are only used to connect between the servers and the port networks (PNs). These two LANs must be private LANs, and carry no other traffic.
  - The duplication interface is a point-to-point LAN that is only used to send information between the two servers.
  - The laptop computer interface is a point-to-point LAN that is used only for local administration and carries no other type of traffic.
  - The enterprise LAN is used for administration and time synchronization. Telephony traffic does not use this LAN. However, in this case, it is possible to subvert this security measure by interconnecting the enterprise LAN NIC with one of the other LANs shown.
- PNs contain additional Ethernet interfaces.

Figure 72: Avaya S8700-series Server with an Avaya MCC1 or an SCC1 Media Gateway on page 234 shows the different LANs that are possible on an S8700-series Server that is configured with Avaya MCC1 or SCC1 Media Gateways along with some of the common adjuncts. The enterprise LAN, adjunct LANs, and agent's LAN can all be connected together to form one network. Or these LANs can be kept physically separate for either traffic reasons or security reasons.

Figure 72: Avaya S8700-series Server with an Avaya MCC1 or an SCC1 Media Gateway



To provide the most secure environment that is possible for the system, network access should be divided into separate zones of control. These zones are sometimes referred to as *DMZs*.

- One VLAN can be administered for administrative traffic, one for call signaling, another for voice bearer traffic, and so on.
- Layer 3 boundary devices (routers, layer 3 switches, and firewalls) should be administered to enforce the corporate security policy on traffic that is destined for the Avaya S8700-series Server, its Avaya MCC1 or SCC1 Media Gateways, or adjuncts.
- Packet filters can permit administrative access only from an administrator's PC and to deny access from the Avaya S8700-series Server or its gateways to the corporate LAN while allowing call signaling and bearer traffic from all IP Telephones appropriate access.

Figure 73: Isolated LANs (Avaya S8700-series Server with an MCC1 or an SCC1 Media Gateway)

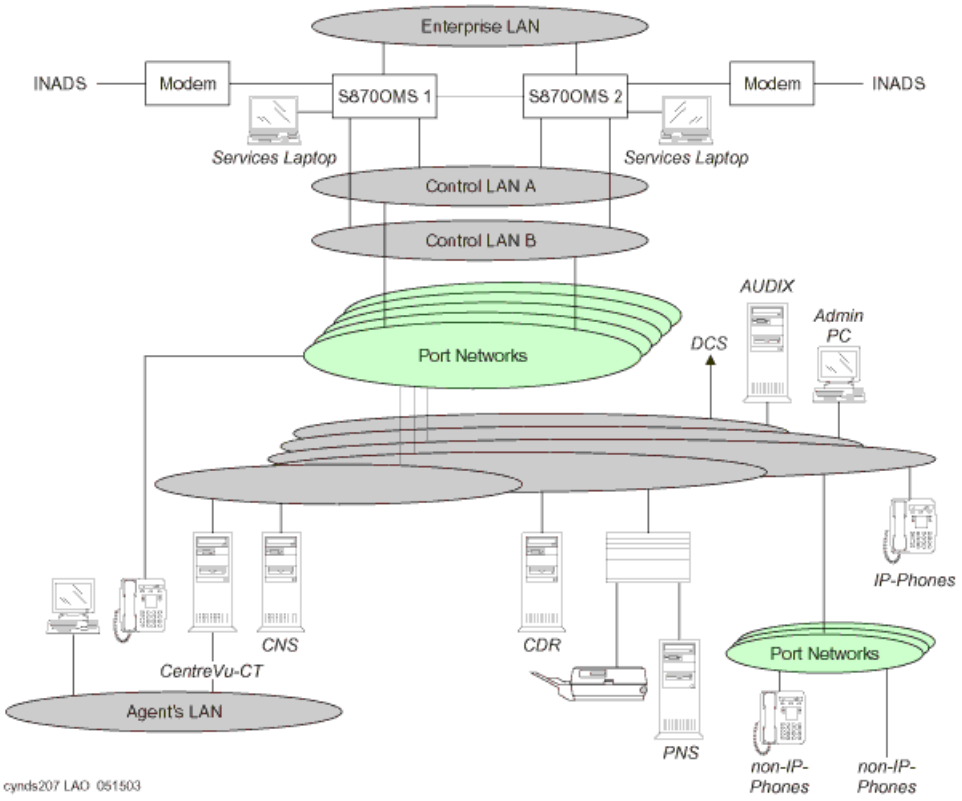


Figure 73: Isolated LANs (Avaya S8700-series Server with an MCC1 or an SCC1 Media Gateway) on page 235 shows how Communication Manager can be configured to allow only certain types of access to specific LAN interfaces on its PNs. For example, even if you connected an administration terminal to one of the other LANs, you cannot get administration access.

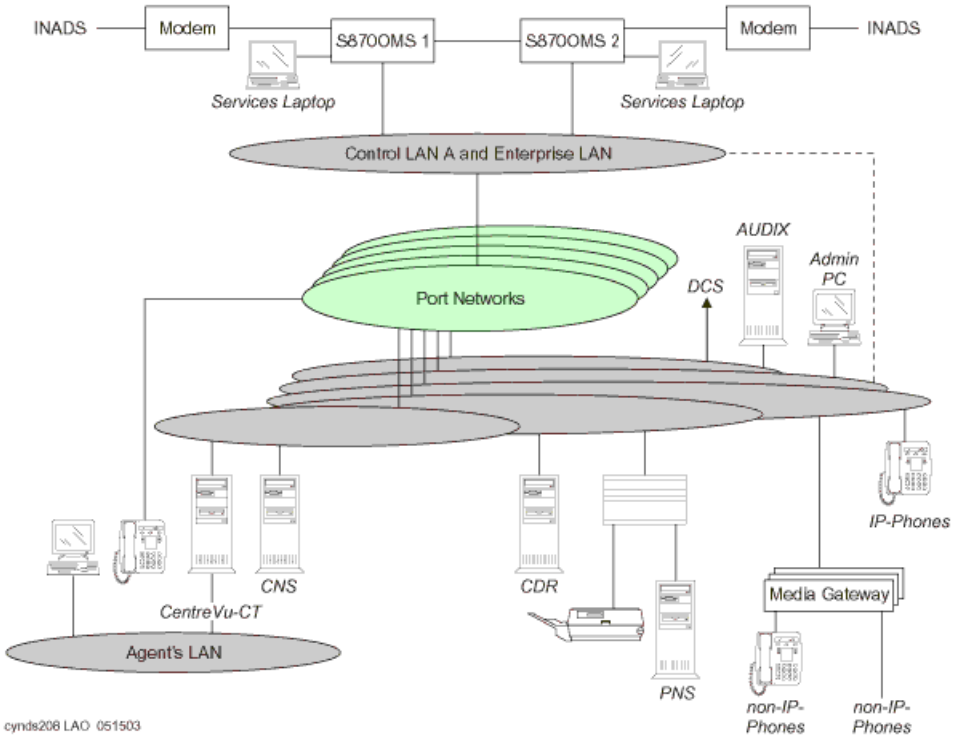
S8700-series Server with Avaya G650 Media Gateways

The S8700-series Server with a G650 Media Gateway also have five interfaces each (Figure 74: Isolated LANs (Avaya S8700-series Server with a G650 Media Gateway) on page 236):

- The enterprise LAN and control LANs are connected together
- There is only one control LAN.
- There are two spare NICs that are not used.

The messages between the S8700-series Server and the G650 are encrypted.

Figure 74: Isolated LANs (Avaya S8700-series Server with a G650 Media Gateway)



Virus and worm protection

Viruses and worms are most often targeted at Microsoft Windows operating systems or such commonly used applications as IIS, Exchange, Outlook, or Word. Because the Avaya S8300, S8400, S8500, and S8700-series Servers are Linux-based and do not interface with these Microsoft products, they have some degree of natural immunity. In addition, viruses and worms are most commonly delivered by e-mail, by visiting infected Web sites, or by sharing disk drives.

The servers do not

- Support incoming email and, therefore, do not forward e-mail
- Contain the Internet Explorer Web browser
- Share drives

All file transfers to the Avaya servers are restricted. Software and service pack files are cryptographically signed to prevent introduction of unwanted software. In addition to this natural immunity, the files and file systems of the Avaya servers are monitored by Tripwire.

Testing

During the development of the S8300, S8500, and S8700-series Servers, or in production of upgrades to its software, Avaya subjects the system to a variety of common “attack tools” to find any overlooked or accidentally created security holes. The exact set of tools that are used varies to keep up with the technology. Common tools include nmap and nessus. Security problems found by these efforts are corrected before the product or the service pack is released.

Environment

Avaya servers are as secure as reasonably possible, consistent with the operational needs of the product and business in which they are used. Security, however, does not end with the servers. These servers are connected to one or more networks that are, in turn, connected to other equipment in the enterprise.

Recommendations for network security

Avaya recommends that these servers be located behind a firewall. Where this firewall is located with respect to other LAN components must be designed on a case-by-case basis. Avaya Professional Services can assist owners in configuring their networks for both security and optimal IP Telephony operation. Other vendors also specialize in this type of consulting. Owners are advised to seek assistance if internal staff is not trained in these areas. Security holes that arise from negligence, ignorance, or oversight or the pressures of schedule or budget are all equally usable by hackers. Malicious activity is a moving target, and what is safe today might not be safe tomorrow. Avaya is committed to providing appropriate secure solutions for its products, and to continuously monitoring evolving security threats. Avaya S8700 and S8300 servers are appropriately secure against the known threats. Avaya responds quickly should new threats appear. Consult these resources for the latest security information:

- Your Avaya account team
- The Avaya support Web site:

  http://www.avaya.com/support

  Click **Security Advisory** in the Technical Database list on the left side of the page.

IP Telephony circuit pack security

Avaya circuit packs such as those in the G650 Media Gateways have a variety of security measures that combine both voice and data security strategies in to a secure package.

The G650 use three different Ethernet interfaces to help isolate the traffic, and protect the specific interfaces that must be secured:

- TN2312BP IP Server Interface (IPSI)
- TN2302AP and TN2602AP Media Processors
- TN799DP Control LAN (C-LAN)

TN2312BP IP Server Interface (IPSI)

Telnet

A telnet service is currently required on the IPSI for manual administration of the IPSI (IP address, default gateway address, VLAN ID, QoS, and Ethernet settings). Telnet access to the IPSI circuit pack is through

- Standard TCP port 23, but only for connections that are physically made through its secondary services Ethernet port. When established, these Telnet accesses are directed to a command menu that supports a variety of administration tasks.
- The OS-debugging shell over port 2312. This port is always available when accessed through the local services port. Telnet access to this port on the control link is opened by a Communication Manager command, and disabled immediately after a session has closed the connection or after 5 minutes of inactivity (see also Control link).

FTP

An FTP service exists, but is disabled by default. Communication Manager must enable the FTP service, and only does so for firmware downloads. Once the FTP service is started, Communication Manager initiates the client-side of the FTP protocol, and then transfers a new firmware file to the IPSI. Once the transfer is complete, the FTP service is automatically disabled. A 5-minute time-out is enforced to guard against cases where the firmware download is started but terminated prematurely. When time-out occurs, the FTP service is disabled until a new command from Communication Manager enables it again.

DHCP

In S8700 fiber-PNC systems only, the IPSI has the ability to receive its IP address information from the S8700-series Server through DHCP. This DHCP service only runs on the control network, and does not connect to a customer's LAN. Avaya has also implemented mechanisms for restricting this DHCP service, so that non-IPSIs do not receive an IP address and IPSIs do not receive an address from a non-S8700-series Server.

Control link

In order to communicate with the S8700-series Server, the IPSI establishes a control link. This link is encrypted through Triple-DES (3DES) by default, although AES is also available. The control link is not open for communication to or from any other entity than the S8700-series Server.

TN2302AP and TN2602AP Media Processors

The TN2302AP IP Media Processor and the TN2602AP IP Media Resource 320 circuit packs are the interfaces to the audio gateway portion of IP Telephony. These circuit packs:

- Use isolated/proprietary operating systems, so they are not susceptible to known viruses.
- Run independently of administrator traffic in order to maintain an isolated security domain, protecting against attacks that exploit trusted relationships.
- Establish audio connections and only respond to a connection when a corresponding signaling connection is established.
- Successfully survive some Denial of Service (DoS) attacks, including SynFlood, and are very resilient to flood-based attacks.

Because of the proprietary operating systems, limited number of open ports, and reliance on UDP sessions, the TN2302AP and TN2602AP are very secure, and are difficult to take out of service. Regardless, the TN2302AP and TN2602AP are completely independent of the administration, maintenance, or reliability of the Avaya Media Gateways, so they cannot be used as “jumping points” to the Media Gateways.

TN799DP Control LAN (C-LAN)

The C-LAN circuit pack interface not only supports signaling for IP Telephony applications, but also supports asynchronous links to INTUITY AUDIX, Call Management System (CMS), and other adjuncts. This interface

- Is independent of the Media Gateway.
- Has no IP link back to the central administration or maintenance processes of Communication Manager.
- Successfully survives DoS attacks created by the SynFlood tools.
- Maintains the IP endpoint RAS authentication sequence, a safeguard against exploiting toll services through IP endpoints.

For more information on the security of Avaya circuit packs, see:

http://support.avaya.com/elmodocs2/multivantage/95933.pdf

Toll fraud

This section contains information about Avaya's design for preventing toll fraud, and includes these topics:

Avaya’s security design

Telecommunications systems face significant and growing problems of theft of customer services. Toll fraud, the unauthorized use of a system and its facilities by a third party, can result in substantial additional charges for telecommunications services.

Avaya makes every effort to assist customers in their battle against “hackers” through the technology that goes into every Avaya product. Avaya Communication Manager is designed with security in mind, and offers many features and capabilities to help maintain security and prevent toll fraud:

- Your company completely controls its communication facilities.
- Your company completely controls its communication’s security policy and features.
- Your company can make immediate changes at any time.

Each new release of Communication Manager addresses customer needs for even greater security capabilities, including enhancements to support the recent changes in the North American Numbering Plan.

Hacking methods

Hackers often facilitate toll fraud activity by gaining access to:

- A system's administration or maintenance port by randomly dialing thousands of telephone numbers, and then attempt to log in using default passwords. Statistical sampling indicates there is a high likelihood that customers still have one or more default passwords in place on their telecommunications system. This allows hackers to completely modify the system to allow toll fraud activity.
- A system’s remote access port, and then use the remote access feature.
- A voice messaging system, and then transfer their calls to outgoing facilities.

To aid in combating these crimes, Avaya continuously works with its customers and supporting law enforcement officials to apprehend and prosecute those criminals.

Your toll fraud responsibilities

No telecommunications system can be entirely free from risk of unauthorized use. But diligent attention to system management and security can reduce that risk considerably. Often a trade-off is required between reduced risk and flexibility. The user and the administrator of the system are in the best position to determine how to tailor the system to meet their mutual needs, while protecting the system from unauthorized use. Under applicable law, customers are responsible for any toll fraud charges that occur. Because you have ultimate control over the configuration and use of the Avaya products and services that you purchase, your company bears the responsibility for fraudulent uses of those products and services. Not only can the financial loss from these calls be substantial, but operational impacts such as reduced productivity can also have an adverse effect.

Toll fraud indemnification

As part of Avaya's ongoing efforts to combat communications fraud and its threat to our business customers, Avaya has introduced an enhancement to its Service Agreement. Beginning January 1, 1996, Avaya indemnifies its customers for charges associated with fraud. This indemnification is available to all customers who are covered by warranty and/or maintain an Avaya Service Agreement for Avaya Communication Manager, INTUITY AUDIX voice messaging, and Avaya Interactive Voice Response systems.

The indemnification enhancement is offered at no additional cost to your service agreement during warranty, or as part of a multiyear Avaya Service Agreement. The only requirement is to follow and maintain the sound security practices that every business should implement. A complete list of these security practices can be obtained from your Avaya Account Team.

Additional toll fraud resources

In an effort to assist customers, Avaya has developed a variety of service offerings and provides materials to assist in helping to identify and combat toll fraud. These offerings and materials include:

- Security Audit Service
- Security Tune-up Service
- Toll Fraud Intervention Hotline
- Avaya Security Handbook

Security Audit Service

The Avaya Security Audit Service is a fee-based, consultation service that provides a security evaluation of a customer's telecommunications system. The Security Audit is conducted by a Avaya team of experts and includes:

1. Preliminary telephone interview
2. On-site or remote security audit of the equipment
3. Analysis of system vulnerability
4. Written recommendations for increasing security

Security Tune-up Service

The Security Tune-up Service is a fee-based, consultative service designed to provide an expedient, online review of the toll-fraud potential in your system. This service is provided for ACM systems and voice messaging systems. Customer support engineers who specialize in security:

1. Remotely access your system.
2. Analyze the potential risks in the system.
3. Optionally implement agreed-upon changes to secure the system.

Toll Fraud Intervention Hotline

If you suspect you are being victimized by toll fraud or theft of services and need technical support or assistance, call the Avaya Toll Fraud Intervention group toll free at

1-800-643-2353 (24 hours a day/7 days a week)

- Consultation charges may apply.
- There is no charge for intervention services performed on equipment that is covered by warranty or service agreement.

Avaya Security Handbook

The *Avaya Security Handbook* summarizes the principal steps that a system administrator can take to reduce the risk of toll fraud. This handbook complements specific documentation for Avaya products and provides a system administrator with a complete, detailed reference for planning and implementing security measures.

Voice quality network requirements

In addition to the influence of the telephony terminals at either end of a connection, there are several network parameters that can affect voice quality. This chapter lists some of the more important ones. The concept of voice quality has different aspects that need to be properly understood and considered. IP Telephony quality can be engineered and administered to several different levels to accommodate differing business needs and budget. Avaya therefore provides network requirements options to allow the customer to choose which "voice quality" level best suits their specific business needs.

Before implementing IP Telephony, Avaya recommends a network assessment to measure latency, jitter, and packet loss to ensure that all values are within bounds.

This section covers the topics:

Network delay

In IP networks, packet delay (latency) is the length of time for a packet to traverse the network. Each element of the network, including switches, routers, WAN circuits, firewalls, and jitter buffers, adds to packet delay.

Delay can have a noticeable effect on voice quality but can be controlled somewhat in a private environment (LAN/WAN). For example, delay can be reduced by managing the network infrastructure or by agreeing on a Service Level Agreement (SLA) with a network provider. An enterprise has less control over the delay when using the public Internet for VoIP.

Previously, the ITU-T recommended 150 ms one-way delay (including endpoints) as a limit for conversations. However, this value was largely misinterpreted as the limit to calculate a network delay budget for connections. Depending on the desired voice quality, network designers might choose to exceed this number for their network.

Some of the issues that must be considered when designing a network for VoIP are:

- One-way delays in excess of 250 ms can cause the well-known problem of "talk-over." This occurs when both parties talk at the same time because the delay prevents them from realizing that the other person has already started talking.
- In some applications, delays less than 150 ms can impact the perceived quality, particularly in the presence of echo.
- Long WAN transports must be considered as a major contributor to the network delay budget, averaging approximately 10-20 ms per 1000 miles. Some transport mechanisms, such as Frame Relay, can add additional delay. Thus, staying within 150 ms, end to end, may not be possible for all types of connections.
- Finally, one-way delay over 400 ms on signaling links between port networks and the S8700-series Server can cause port network instability.

Again, there is a trade-off between voice quality and the technical and monetary constraints which businesses confront daily. For this reason, Avaya suggests the following guidelines for one-way LAN/WAN delay between endpoints, not including IP phones:

- 80 ms (milliseconds) delay or less yields the best quality.
- 80 ms to 180 ms delay can give Business Communication quality. This delay range is much better than cell-phone quality if echo is properly controlled and, in fact, is very well suited for the majority of businesses.
- Delays exceeding 180 ms might still be quite acceptable depending on customer expectations, analog trunks used, codec type, and the presence of echo control in endpoints or network equipment.

The Converged Network Analyzer (CNA) system is capable of providing ongoing measurements of network delay (see CNA Application Performance Rating on page 254). CNA will also generate alarms when network delay rises to levels that are detrimental for voice quality. For more information on CNA, see The Converged Network Analyzer on page 344.

Codec delay

In addition to delay incurred in the network, codecs in the endpoints also add some delay. The delay of the G.711 codec is minimal. However, the G.729 codec, for example, adds:

- approximately 10 ms of algorithmic delay in each direction
- another 5 ms look-ahead
- plus signal processing delays.

The compression algorithm in G.723.1 uses multiple blocks (called frames) of 30 ms voice samples per packet. This results in increased latency over codecs configured to use 20 ms or less samples per packet.

The G.722 codec adds a 0.82 ms delay.

Jitter

Jitter is thought of as the statistical average variance of the arrival time between packets received from the IP network. To compensate for jitter, a de-jitter buffer is implemented in VoIP endpoints. The purpose of the jitter buffer is to hold incoming packets for a specified period of time such that voice samples can be played out at a regular rate to the user. In doing so, the jitter buffer also adds packet delay.

Excessive jitter might cause additional delay if the jitter still fits the size of the jitter buffer. Excessive Jitter might also result in packet discard creating audible voice-quality problems when the variation is greater than the jitter buffer size. Dynamic jitter buffers give the best quality. Static jitter buffers should generally be sized at twice the largest statistical variance between packet arrivals. However, care needs to be taken in the design of the resizing algorithm of dynamic buffers in order to avoid adverse effects. Dynamic jitter buffering can exacerbate problems in an uncontrolled network. The network topology can also affect jitter. The existence of multiple paths between endpoints with load balancing enabled in routers can contribute significant amounts of jitter.

The following Avaya products all have dynamic jitter buffers to minimize delay by automatically adjusting the jitter buffer size:

- Avaya G350 and G700 Media Gateways and G650 Medial Gateways with the TN2302AP circuit pack
- Avaya IP SoftPhone software
- Avaya 4600 Series IP Telephones

On a VoIP network, the Avaya Converged Network Analyzer (CNA) system is capable of providing ongoing measurements of jitter (see CNA Application Performance Rating on page 254). CNA can also generate alarms when jitter rises to levels that are detrimental for voice quality. For more information on CNA, see The Converged Network Analyzer on page 344.

Packet loss

Packet loss occurs when packets are sent but not received, or are received too late to be processed by the endpoint jitter buffer. Too much delay or packet mis-order can be perceived as lost packets. It may appear that the network is losing packets when in fact they have been discarded intentionally because of late arrival at the endpoint. IP networks are characterized by unintentional packet loss in the network as well as by discarded packets in the jitter buffers of the receiving endpoints.

The effects of packet loss on VoIP service are multifold:

- Problems caused by occasional packet loss are difficult to detect because each codec has its own packet loss concealment method (PLC). Therefore, it is possible that voice quality would be better using a compression codec (G.729A), which includes its own PLC, compared to a full bandwidth G.711 codec without PLC.
- Packet loss is more noticeable for tones (other than DTMF) than for voice. The human ear is less able to detect packet loss during speech (variable-pitch), than during a tone (consistent pitch).
- Packet loss is more noticeable for contiguous packet loss than for random packet loss over time. For example, the effect of losing ten contiguous packets is worse than losing ten packets evenly spaced over an hour time span.
- Packet loss is generally more noticeable with larger voice payloads per packet than with smaller packets, because more voice samples are lost in a larger payload.
- In the presence of packet loss, the time for a codec to return to normal operation depends on the type of codec.
- Even small amounts of packet loss can greatly affect a TTY/TDD device's (for hearing-impaired people) ability to work properly.
- Packet loss for signaling traffic increases network traffic substantially when the loss exceeds 3%, possibly impacting voice quality.

Network packet loss

Like packet delay, Avaya offers customers a tiered approach of recommendations to deal with network packet loss to balance new network costs and the constraints of business directives.

The maximum loss of IP packets (or frames) between endpoints should be:

- 1% or less for best quality.
- 3% or less for Business Communications quality. Again, this quality is much better than cell-phone quality.
- More than 3% may be acceptable for voice but may negatively impact signaling, which might degrade voice quality due to increased traffic. More information on signaling bandwidth requirements can be found in white papers on the Avaya Support website.

The Converged Network Analyzer (CNA) system is capable of providing continuous measurements of network packet loss (see CNA Application Performance Rating on page 254). CNA can also generate alarms when network packet loss rises to levels that are detrimental for voice quality. For more information on CNA, see The Converged Network Analyzer on page 344.

Avaya’s VoIP Monitoring Manager (VMM) can measure packet loss for ongoing calls. The Agilent (HP) Internet Advisor, Finisar's Surveyor Explorer, Radcom's Prism, NAI's Sniffer, and others also measure packet loss.

Packet loss concealment (PLC)

Some packet loss can be dealt with by attempting to conceal the loss by generating voice samples to take the place of the missing samples. ITU standards G.711 Annex I and the G.729 standard define methods by which packet loss concealment can be provided. Excessive packet loss cannot be disguised so, ultimately, PLC gives way to comfort noise generation (CNG) if too many packets are lost in succession.

Ramping down to silence is a typical way that PLC is performed. Loss of six consecutive packets is considered to be the maximum number of packets over which PLC can be sensibly applied.

Echo

The two main types of echo are acoustic echo and electrical echo caused by hybrid impedance mismatch. Usually, in a 2-party call, only the speaker hears an echo but the receiver does not. However, in a conference call many parties might hear an echo.

Acoustic echo occurs when a talker’s voice traverses through the airpath in the acoustic environment of the receiver and feeds back to the microphone of the rereceiver’s terminal. The severity of the echo effect depends on the acoustic properties of the remote room. For example, room size and wall reflection characteristics.

Electrical echo is also a reflection effect but is due to an impedance mismatch between four-wire and two wire systems or in the interface between a headset and its adapter.

The user's perception of echo increases with delay. In practice, most echo received within 30 ms is ignored by the human auditory system. However, if the level of the received echo signal is extremely high, even a couple of milliseconds delay will cause adverse perception of echo. Echo received after 30 ms will generally be perceived as an annoyance. Because of the end-to-end latency in some IP Telephony implementations exceeds the latency in some circuit-switched systems, the perception of echo can be greater in the IP Telephony system.

One strategy for dealing with echo is the deployment of echo cancellers at strategic places in phones or network equipment. Echo cancellers, which have varying amounts of memory, store incoming voice streams in digital form in a buffer and compare the received voice with the previously transmitted voice patterns stored in memory. If the patterns match, the canceller considers it an echoed signal and attempts to remove it.

Because echo cancellers are not perfect, there is a residual level of echo left even in optimal operating conditions. Echo cancellers operate properly only if the one-way delay between the echo canceller and the echo source (for example, the acoustic airpath at the telephone set or electrical hybrid) is larger than the echo canceller can handle, the echo canceller will not find a pattern to cancel.

Avaya's G350 and G700 Media Gateways, the Avaya MM760 VoIP Media Module, the Avaya TN2302AP IP Media Processor (in the G650 Media Gateways), the Avaya TN2602AP IP Media

Resource 320, the Avaya IP SoftPhone, and the Avaya 4600 Series IP Telephone all incorporate echo cancellation designed for IP Telephony to improve voice quality.

Signal levels

In order to provide more natural-sounding conversations, voice communication systems attempt to emulate a typical communication scenario where the two parties are speaking directly and are separated by one meter. To achieve these conditions, an acoustic loss of 10dB is added between speaker and listener. Any significant differences from this loss level will be audible as a signal level that is either too soft or too loud and thus may result in some degree of listener discomfort.

In IP Telephony networks, the end-to-end loss of 10 dB is implemented as 8 dB in the speaker's telephone, 0 dB in the IP network, and another 2 dB loss in the listener's telephone. To account for personal preferences or the presence of background distortions, listeners may adjust relative to the 10 dB loss value by adjusting the volume control of their telephone. The IP Telephony loss values are globally identical and specified in ITU-T Recommendations.

In traditional circuit-switched networks the telephone transmit, receive, and inter-port line/trunk losses are country-dependent. The end-to-end country-specified losses often also differs somewhat from the 10dB loss value for historical reasons. The country-dependency of loss values makes it more challenging to guarantee a proper listener signal level when the PSTN is involved or when country borders are traversed.

IP Telephony gateways should provide proper signal level adjustments in the direction from the IP network to the circuit-switched network and in the reverse direction, and also between circuit-switched ports.

To allow for multi-country deployment of Avaya telephones and gateways, these devices facilitate programmable loss values. In order to ensure that the signal levels are controlled properly within the scope of a voice network consisting of Avaya systems, the appropriate country-dependent loss plan should be administered.

In addition to administering loss for two-party calls, Communication Manager allows country-dependent conference call loss administration. Loss is applied depending on the number of parties involved in the conference.

Echo and Signal Levels

As mentioned before, in circuit-switched telephony, echo may be caused by acoustic reflection in the remote party's environment, or by electrical reflection from 2-to-4 wire analog hybrid impedance mismatches. Impedance mismatch can occur in analog telephones and analog line/trunk cards, electrical cross-talk in circuitry, or in telephony wiring (particularly in low-cost headsets). For this reason, in circuit-switched analog and digital phones, a relatively large transmit loss is implemented in order to minimize the perceived echo due to electrical reflection and cross-talk effects. In principle, the transmit loss of telephones could be made very large followed by signal amplification in the receiving telephone. In practice however, the transmit loss should be limited to prevent the electrical voice signal from dropping below electrical background noise. This has resulted in the adoption of transmit loss and receive loss values around 8 dB and 2 dB, respectively, although country-specific values may actually deviate quite significantly from these values.

The loss plan administration provided by Avaya Communication Manager software is primarily intended to control signal losses in telephones and gateways, and not intended to control echo. However, in case of severe echo, the administered loss can be changed to a different plan. In general, an increase of the loss between two endpoints by a certain amount will decrease the echo level by twice this amount. It is not advised to use loss plan administration in this way without consultation with Avaya Services personnel. It is better to reduce the echo by using Avaya products with echo cancellers to minimize echo.

Tone Levels

The level of call progress and DTMF tones played out through telephones must adhere to specified levels in order to be satisfying for the average user. Again, respective standards are country specific and can be set in Communication Manager by administration. The volume of received call progress tones can be adjusted by the telephone volume control.

Codecs

Codecs (Coder-Decoders) convert between analog voice signals and digital signals. Avaya supports several different codecs offering varying bandwidth usage and voice quality, including the following codecs:

- G.711 produces uncompressed audio at 64 kbps
- G.729 produces compressed audio at 8 kbps
- G.723.1 produces compressed audio at 5.3 or 6.3 kbps
- G.722 produces compressed audio at 64, 56, or 48 kbps

Table 46 provides a comparison of voice quality considerations associated with some of the codecs supported by Avaya products.

Toll-quality voice must achieve a MOS (Mean Opinion Score) of 4 or above. The MOS scoring is a long-standing, subjective method of measuring voice quality.

Table 46: Comparison of speech coding standards (without IP / UDP / RTP overhead)

Standard	Coding Type	Bit Rate (kbps)	MOS-LQO[1,2] (Mean Opinion Score - Listening Quality Objective)
G.711	PCM	64	4.37
G.729	CS-ACELP	8	3.94
G.723.1	ACELPMP-MLQ	6.3 5.3	3.78 3.68

1. As predicted. Measured according to ITU-IT Recommendation P.862 (PESQ). See draft Recommendation P.862.2, application guide for PESQ.
2. Given MOS-LQO values for American English.

Because it does not use compression, G.711 offers the highest level of voice quality assuming proper operation of the IP network. Unfortunately, there is a trade-off with higher bandwidth usage. In situations where bandwidth is scarce, such as across WAN links, G.729 offers a good compromise with lower bandwidth usage, but still good fidelity audio.

In general, compression codecs use twice as many signal processing resources than the G.711 codec. On the TN2302AP (Media Processor) circuit pack (and on the G700 VoIP engine) there are 64 DSP resources. Thus, the number of calls supported by one Media Processor board or G700 is:

- 64 G.711 calls
- 32 compressed calls (for example, G.729)
- Some number in-between for a call mix.

The formula for calculating the number of calls one Media Processor board supports is

$$(\text{Number of uncompressed calls}) + 2 \times (\text{Number of compressed calls}) \leq 64$$

The TN2602AP circuit pack supports:

- 320 channels of G.711 (u/a-law)
- 320 channels of G.729A/G.729AB
- 320 channels of G.726 (32 kbps only)
- 320 channels of T.38

- 320 channels of V.32 SPRT

The above channel counts are the same if AES encryption and SHA-1 authentication are enabled.

The One-X Deskphones (96xx) support the G.722 codec with 64 kbps and with 20 ms packets

Generally, G.711 is used on LANs because bandwidth is abundant and inexpensive whereas G.729 is used across bandwidth-limited WAN links.

G.726 Codec and H.248 Media Gateways

As of Communication Manager release 3.1, media processing resources on H.248 Media Gateways support the G.726 codec. The following table provides the corresponding capacities:

Table 47: Number of Simultaneous Bi-Directional Connections Supported

Codec	G250	G350	G700
G.726A Unencrypted	10	16	32
G.726A with AEA Encryption	10	16	32
G.726A with AES Encryption	10	12	24

Silence suppression/VAD

Voice Activity Detection (VAD) or silence suppression can also be used to save bandwidth. During a conversation, because only one party is speaking at any given time, more than 40% of the transmission is silence. Voice Activity Detection (VAD) in Avaya IP telephones monitor the locally produced voice signal for voice activity. When no activity is detected for the configured period of time, packets are no longer transmitted. This prevents the encoder output from being transported across the network when there is silence, resulting in bandwidth savings.

When silence suppression is enabled, the remote end is instructed to generate "comfort noise" when no voice is present to make the call sound more natural to users. The trade-off with silence suppression lies with the silence detection algorithm. If it is too aggressive, the beginnings and ends of words can be "clipped." If not aggressive enough, no bandwidth is saved.

Silence suppression is built into G.729B. It can be enabled for other codecs from within Communication Manager. Because of voice quality concerns with respect to clipping, silence suppression is generally disabled (with the exception of G.729B).

The following Avaya products employ silence suppression to preserve bandwidth:

- Avaya Communication Manager software (for control)

- Avaya 4600 series IP Telephone
- Avaya IP SoftPhone
- Avaya Media Gateways

For procedures to administer QoS parameters, refer to *Administration for Network Connectivity for Avaya Communication Manager* (555-233-504).

Transcoding/tandeming

Transcoding or tandeming occurs when a voice signal passes through multiple codecs. This can be the case when call coverage is applied on a branch office system back to a centralized voice mail system. These calls might experience multiple transcodings including, for example, G.729 across the WAN and G.723.1 into the voice mailbox. Each transcoding action results in degradation of voice quality. Transcoding can be minimized by using the Communication Manager feature called DCS with Rerouting (Path Replacement). This feature detects that the call coming through the main switch has been routed from one tandem switch, through the main, and back out to a third switch. In these cases the system re-routes the call, replacing the path through the main system with a more direct connection. Avaya products minimize transcoding. "Shuffling" and "hairpinning" also reduce transcoding. For more information, see Hairpinning on page 201 and Shuffling on page 201.

CNA Application Performance Rating

The Avaya Converged Network Analyzer (CNA) system is a network optimization solution that can be configured to improve the Internet experience of customers and local network users, improve the speed and reliability of Internet VPN connections, and optimize cost of service.

Reporting on low level measurements, such as delay, jitter, and packet loss, is important and helps predict trends and debug networking related issues that are affecting an application. In addition to low level measurements, CNA provides an Application Performance Rating (APR) that translates low level statistics in to a 0 to 5 metric that summarizes the effect of all low level scores into one score. This APR score allows users, by looking at one number, to determine whether their application performance is acceptable at any given time. CNA also uses APR scores to derive network availability from the point of view of the application.

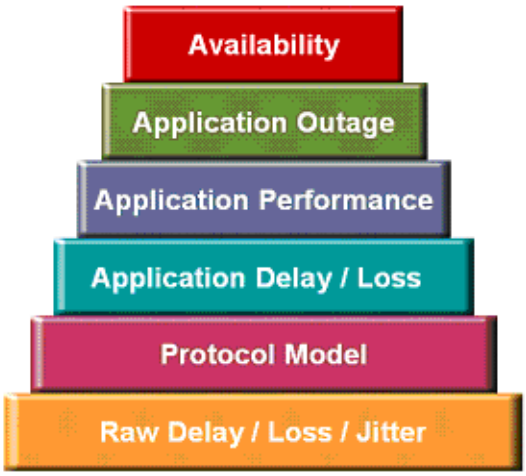
For more information on CNA, including system requirements, licensing, and configuration, see *Converged Network Analyzer Fundamentals Guide,* 14-601298.

Translating low level statistics to an Application Performance rating

The CNA assessment of application performance is based on application models, which convert the raw delay, jitter, and loss measurements into an application performance rating that ranges from 0 to 5. This rating is normalized across applications. Application models are tailored to different applications, including VoIP, and take into account the specific characteristics and requirements of the various applications.

CNA Application Models follow a five-stage methodology, shown in Figure 75.

Figure 75: Converting raw statistics into an application performance rating



From the bottom, the five steps include:

- The measurement of low-level network parameters such as latency, loss, and jitter for each available path between locations.

The computation of transport delay from the raw scores; this takes into account the distinct characteristics of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), and thus assesses the impact on applications in general, not taking specific application sensitivities into consideration.

- The computation of application delay, specifically the transaction between the two end points.
- The determination of an application performance rating, using a ranking from one to five stars, similar to movie ratings.
- Finally, the time periods where the voice quality is determined to be unacceptable are logged as “bad minutes” for that path. Adding up the bad minutes allows CNA to compute the effect of network problems on application availability

Available application models

Voice

The voice model converts low level statistics (network delay, latency, and loss) into an APR score that takes into account voice requirements. Given the sensitivity of voice to jitter, the voice model is especially sensitive to jitter. This model is also very sensitive to sustained loss, which effect can be detrimental to voice. This model is also sensitive to delay and loss. (See Section 3 for a detailed description of the effect of delay, jitter, and loss on voice quality).

Video conferencing

The video conferencing model converts low level statistics into an Application Performance Rating (APR) score that takes into account video conferencing requirements. Given the detrimental effects of loss on video conferencing, this model is very sensitive to loss. This model is also sensitive to jitter and latency.

Enterprise model

The enterprise model takes into account the effect of low level network characteristics on short TCP transactions. This model is very sensitive to network loss. On the other hand, this model is not affected by jitter. Given that signaling traffic uses TCP and consists of short transactions, The CNA application model that best captures the characteristics of signaling traffic is the enterprise application model.

Web model

The web model is best suited for web applications. It converts latency and loss measures into an APR score that best describes the user experience in the context of a typical web transaction.

For more information on CNA, see The Converged Network Analyzer on page 344.

Avaya Integrated Management

This chapter outlines Avaya's system, network, and device management and monitoring products, and some common third-party tools. It also discusses the distributed and centralized management models, and describes how Avaya management products fit into those models.

Integrated Management overview documents

The following overview documents describe the Avaya Integrated Management offers:

- *Integrated Management Release 4.0 Overview*, 14-601718, Issue 1, March 2007
- *Integrated Management for Distributed Office Release 4.0 Overview*, 14-601538, Issue 1, April 2007

Avaya Integrated Management offers

Avaya Integrated Management provides a comprehensive set of tools that enables you to manage converged voice and data networks with ease and efficiency. The Avaya Integrated Management applications include the tools that enable you to

- configure, monitor, and optimize the performance of Avaya servers, gateways and endpoints
- monitor voice over IP traffic
- manage Quality of Service (QoS) policies
- control network quality

Administration Tools Offer

Administration Tools is a Microsoft Windows solution for Avaya Integrated Management. It is designed for small-to-medium size networks that run Microsoft Windows platforms. The Avaya Integrated Management applications provided in this offer are as follows:

- Avaya Site Administration
- Avaya Voice Announcement Manager

See Chapter 2: Avaya Integrated Management Applications on page 15 for a description of each application.

In Integrated Management Release 3.1 or later, Avaya Voice Announcement Manager enables you to use an SCP server for secure file transfer to G250 and G350 media gateways. These media gateways have an SCP client. You can either use an existing SCP server or install OpenSSH SCP Server from the Administration Tools CD.

When you install OpenSSH SCP Server from the Administration Tools CD, the SCP server is installed on the same PC as the Administration Tools applications. During OpenSSH SCP Server installation, you are able to select Windows users on that PC and configure them as users for the SCP server. When SCP users log on to the PC, they are automatically logged on to the SCP server as well.

The Administration Tools offer provides one user license. Customers can purchase an option that is for up to five Avaya Communication Managers and provides up to five user licenses. Another option is available that provides unlimited client licenses for Avaya Site Administration and Avaya Voice Announcement Manager. However, these licenses are restricted to a single campus (geographic area) or country.

VoIP Monitoring Management Offer

The VoIP Monitoring Management offer provides Avaya VoIP Monitoring Manager as a stand-alone application to provide flexibility in combining multiple offers to meet your requirements.

Avaya VoIP Monitoring Manager is a VoIP Quality of Service (QoS) monitoring tool. It enables you to monitor and review the quality of a call on an Avaya VoIP Network. Avaya VoIP Monitoring Manager allows you to search endpoints, view reports, export reports, and generate automatic alarms. See VoIP Monitoring Manager on page 22 for more information about his application.

The VoIP Monitoring Manager offer provides one license for up to 2000 endpoints and 40 gateways. Customers can purchase an option that is for an additional 2000 endpoints and 40 gateways. Another option is available that provides unlimited licenses. However, these licenses are restricted to a single campus (geographic area) with VoIP Monitoring Manager installed on one server.

Enterprise Network Management Offer

Enterprise Network Management is a Microsoft Windows solution for Avaya Integrated Management. It is designed for VoIP networks of any size that run Microsoft Windows platforms.

It provides a complete converged solution that helps you manage your network through a common web-based user interface. This offer provides the ability to see your whole voice system structure and hierarchy. You are able to administer and manage Avaya voice systems and Avaya converged devices (such as media gateways and servers).

The Avaya Integrated Management applications provided in this offer are as follows:

- Network Management applications:
  - Avaya Network Management Console with System View
  - Avaya Provisioning and Installation Manager
  - Avaya Network Configuration Manager
  - Avaya Software Update Manager
  - Avaya SMON Manager (90-day trial) ñ Customers can purchase the license key to activate the SMON Manager beyond the 90-day trial.
  - Avaya Secure Access Administration
- Avaya Device Managers:
  - Avaya G350/G250 Manager
  - Avaya P330/G700 Manager
  - Avaya C360 Manager

In Release 3.1 or later, OpenSSH SCP Server is an additional component installed on the Windows server so that Avaya Software Update Manager can use this SCP server for secure file transfer.

See Chapter 2: Avaya Integrated Management Applications on page 15 for a description of each application.

The Enterprise Network Management offer provides one server license for the Avaya Network Management Console and the provisioning tools including Software Update Manager.

System Management Offer

System Management is the premier solution to manage large converged networks. This offer includes the Avaya Integrated Management advanced management tools, which run on Red Hat Linux. System Management also supports HP OpenView on Microsoft Windows. Combined with Enterprise Network Management Release 4.0, you have the full complement of products to administer the myriad of features in the Avaya Communication Manager; monitor your entire

voice and data network from a central location; and manage the Avaya network server and IP endpoints.

Note:

The most current release of the System Management offer is Release 3.2. System Management Release 3.2 applications are compatible with the applications in the Avaya Integrated Management Release 4.0 offers.

The Avaya Integrated Management applications provided in this offer are as follows:

- Avaya MultiSite Administration
- Avaya Proxy Agent
- Avaya Fault and Performance Manager
- Avaya Integrated Management Database
- Network Management System Integration (NMSI) for Windows

See Chapter 2: Avaya Integrated Management Applications on page 15 for a description of each application.

Third-party network management products

This section describes some third-party monitoring tools that might provide benefit to companies implementing IP Telephony. Avaya is not involved with the development of these products. Inclusion on this list is not exhaustive, nor does it represent an endorsement from Avaya. Products are listed here as a convenience for our customers.

Multi Router Traffic Grapher

The Multi Router Traffic Grapher (MRTG) monitors the traffic load on network links, and generates HTML pages of graphic-displayed images that provide a live visual representation of this traffic. MRTG is based on Perl and C, and works under UNIX and Windows NT. The Multi Router Traffic Grapher:

- Uses SNMP to read the traffic counters of your routers, logs the traffic data, and creates graphs that represent the traffic on the monitored network connection. These graphs are embedded into Web pages. MRTG even allows you to accumulate two or more data sources into a single graph.
- Creates visual representations of the traffic seen daily, during the last week, the last month, and the last year. MRTG performs well enough to monitor 200 or more network links from any reasonably-performing PC.

- Monitors any SNMP variable that you choose. You can even use an external program to gather the data that MRTG should monitor, for example:
  - System load
  - Login sessions
  - Modem availability

For more MRTG information, see:

- http://www.mrtg.org for the main MRTG Web site. Their product is available free of charge under the terms of the GPL.
- http://www.ee.ethz.ch/stats/mrtg/ for an example.

HP OpenView Network Node Manager

HP OpenView Network Node Manager (NNM) and Network Node Manager Extended Topology together provide your management team with the capabilities that you need to address your key business and network challenges:

- A new approach to root-cause analysis that includes a set of easy-to-use tools to help you identify and resolve conditions before they become problems.
- ID for Networks delivers advanced capabilities for network event reduction, root-cause analysis and a new management concept called State Analysis, which actively determines the health of network protocols and complex network configurations.
- Includes out-of-the-box correlators for enhanced root-cause analysis and the new Correlation Composer to easily tailor the out-of-the-box correlators that are shipped with Network Node Manager to fit your particular needs.
- The NNM serves as a SNMP manager, trap collector, and connectivity tester. It also acts as a framework for the attachment of other programs, such as Avaya Network Management Console with VoIP SystemView.
- Topology discovery visually shows the interconnection of routers, switches, and endpoints.

Network management models

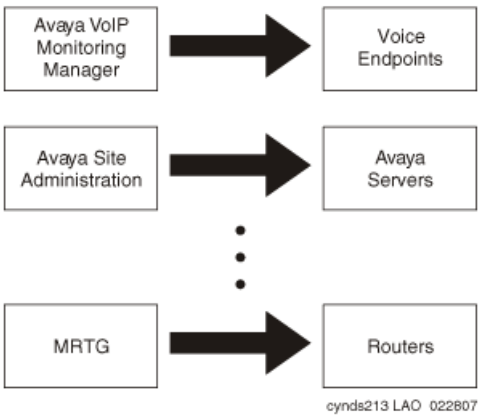
There are two basic network management models:

- Distributed — specialized, nonintegrated tools, and sometimes organizations, to manage discrete components.
- Centralized — integrated network management tools and organizations for a more coherent management strategy.

Distributed (component)

Distributed network management is the default management model for network equipment. As Figure 76 shows, each device is managed separately, and can have its own management interface. There is no commonality between these interfaces. Some might be CLI-based, Web-based, or GUI-based applications. In addition, third-party tools such as MRTG complement integrated management interfaces to provide additional functionality.

Figure 76: Tools for distributed network management



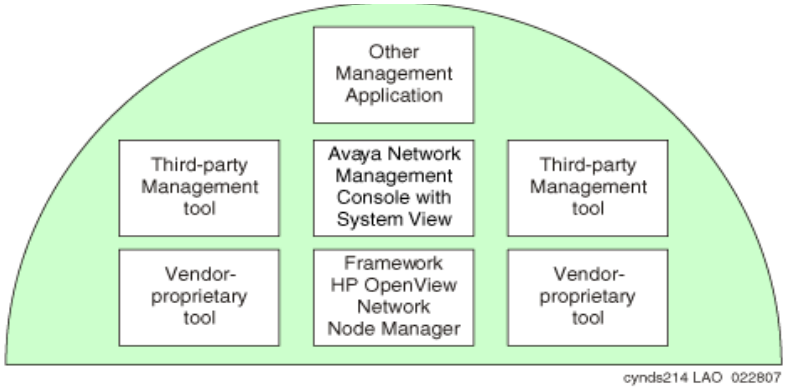
The advantage to this model is that the cost of tools is low compared to the centralized model. Many of the tools are included with the purchase of networking equipment, and many are open source. Also, many of these tools are more specialized on a specific platform or task than centralized management tools. Most Avaya Integrated management products, including Avaya VoIP Monitoring Manager, fall into this category.

There are numerous disadvantages to this model. First, this model requires more support personnel than the centralized model. Next, there are numerous interfaces that support staff must learn, which greatly increases training costs. Finally, the support person must check many places to get the full status of the network, which adds time and the likelihood of missing critical data. This model is appropriate in small to medium-sized enterprises with relatively few pieces of network equipment. It is not appropriate for most large enterprises or enterprises with complicated networks.

Centralized (hybrid)

The centralized management model strives to make all network management available in a central location. It generally begins with a framework product such as HP OpenView NNM. This framework product serves as an SNMP trap receiver for alarm data sent by networking devices. It also provides network topology discovery and availability testing.

Figure 77: Centralized management model



Additional management tools, such as Avaya Network Management Console with VoIP SystemView, attach to the framework (Figure 77). They can be launched directly from the underlying application, and can share data with it. This allows a network administrator to go to a central location for most network management and configuration tasks. Client devices are configured to send alarm and event data to the centralized manager, generally through SNMP. The management station also has the ability to periodically poll the client for specific information. This can be used to graph performance, for example. Polling can also be used for inventory management.

There are many advantages to this model:

- Because a centralized location is used, fewer administrators are required to manage a network.
- Administrators are more likely to catch critical information because it is all in one place.
- Administrators need to learn fewer interfaces, which reduces training costs.
- More advanced centralized management products offer event correlation, which increases the likelihood of proactively catching a problem before it adversely affects users.

The disadvantage to the centralized model is cost. Typically, centralized management tools cost more than distributed tools. In addition, the implementation and integration can be complex. Finally, the enterprise must adjust the manager as the network changes. If the management server is not actively maintained, it quickly falls into disuse.

In practice, it is rare for an enterprise to completely embrace the centralized model. Some applications may not “bolt on” to a particular framework, for example. Also, sometimes an enterprise writes a “homegrown” application to cover an outage with the management server. In addition, the distributed model is useful for times when the central management tool is unavailable.

This resulting hybrid management model that combines elements of centralized management with distributed management tools is most appropriate for large enterprises, or enterprises with complex networks. It is also appropriate for smaller enterprises that can justify the cost of the tools and have in-house expertise to keep the system running.

Reliability and Recovery

The purpose of this chapter is to provide the reader an overview of the subject of communication-system “availability,” specific to Avaya Communication Manager and Avaya servers and gateways. The discussion that follows demonstrates Avaya’s long-standing commitment to high availability in hardware and software design and the architectural strength of Avaya Application Solutions.

A brief description of availability and its significance to a communications system is provided. Hardware-design considerations, software-design and recovery considerations, IP Telephone and remote media gateway recovery, and overall maintenance strategy are also described. The reliability tables specify the reliability performance of Avaya Application Solutions building blocks.

This chapter contains information on these topics:

Reliability

Customers need the full reliability of their traditional voice networks, including feature richness and robustness, and they want the option of using converged voice and data infrastructures. With the convergence of voice and data applications that run on common systems, a communications failure could bring an entire business to a halt. Enterprises are looking to vendors to help them design their converged infrastructure to meet their expected availability level.

“High availability” communications require the system to work reliably with pre-existing transport infrastructures, and to integrate with a wide variety of external connectivity options. As a result, the underlying architecture should be designed to support reliable performance at every level. Avaya Communication Manager running on the Avaya S8700 and the 8300 Servers employs a variety of techniques to achieve this high reliability and availability.

Communication Manager is designed to automatically and continually assess performance, and detect and correct errors as they occur. The software incorporates component and subassembly self-tests, error detection and correction, system recovery, and alarm escalation paths. Its maintenance subsystem manages hardware operation, software processes, and data relationships.

Employing the TCP/IP packet-based transport architecture allows additional reliability advantages. One example is the load-sharing and fail-over ability of the principal IP resources found in the media gateways. The TCP/IP architecture also allows telephones to have a recovery mechanism of their own, so they can connect to alternate controllers if the link to their primary gatekeeper is broken.

For large systems, Avaya S8700-series Servers provide server redundancy, with call preserving fail-over, on the strength of a Linux operating system. With Enterprise Survivable Servers farther enhancement is provided to ensure business continuity in the event of connection failure or events leading to total failure of main server complex, such as natural disaster.

The Avaya S8300 and S8500 Servers can further enhance redundancy by serving as Local Survivable Processors (LSPs) for H.248 Media Gateways within networks. LSPs can take over segments that have been disconnected from their primary call server, and provide those segments with Avaya Communication Manger operation until the outage is resolved.

For more information about availability assessment and methodologies, see

- The White Paper, *Avaya Communication Manager Software Based Platforms: High Availability Solutions, Avaya Media Servers and Gateways.*

  High_Availability

- The Tolly Group White Paper, *Building Survivable VoIP for the Enterprise*

  Survivable_VoIP

- The previous version of this book, *Avaya Application Solutions: IP Telephony Deployment Guide*, Issue 4.3.

  IPTDG_4_3

Use the indicated links to access these documents on the Avaya Support web site.

Survivability solutions

Avaya Communication Manger release 3.0 introduces new features in support of enhancing high availability and survivability. These features are in support of business continuity through unscheduled outages such as network failure and congestion as well as scheduled outages such as server upgrades.

General survivability features:

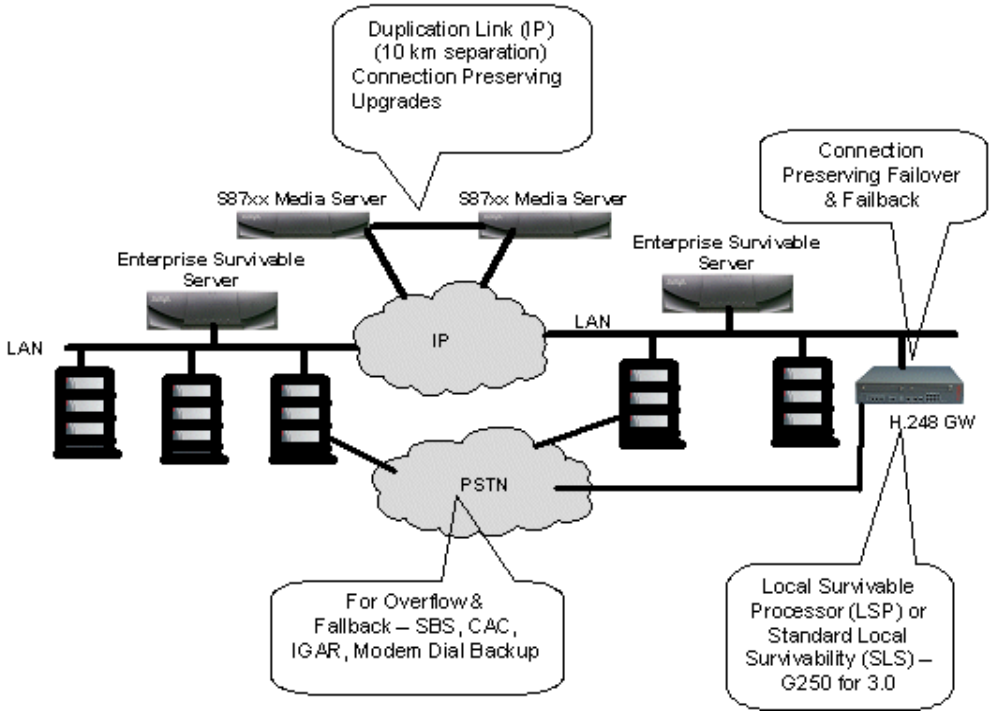
- S8700-series server separation
- Enterprise Survivable Server (ESS)
- Connection preserving upgrades for duplex servers
- Inter-Gateway Alternate Routing (IGAR)

Survivability for branch office media gateways:

- G700/G350 Media Gateway recovery via LSP
- Modem dial backup
- Auto fallback to primary Communication Manager for H.248 media gateways
- Connection-preserving failover for H.248 gateways
- G250 Media Gateway local survivability function (SLS)

Figure 78: Release 3.0 system example on page 268 summarizes these enhancements:

Figure 78: Release 3.0 system example



S8700-series Server Separation

S8700-series server separation allows the two servers in an S8700-series Server pair to be geographically separated up to a maximum distance of 10 kilometers over a fiber-optic link. Separating the servers offers an improved survivability option by allowing servers to reside in two different buildings across a campus or small Metropolitan Area Network. This feature capability is applicable to the S8700-series Servers in both fiber-PNC and IP-PNC configurations.

The sever separation feature works best when each server is accompanied by its own Layer 2 Ethernet switch. For example, in a fiber-PNC system, each server would have an Ethernet switch co-located with it. The two Ethernet switches would be connected using a 100base-FX or Gigabit Ethernet link. For optimum results, the port networks should also be distributed with respect to Ethernet switches.

Note:

S8700-series Server Separation does not provide for separation of duplicated center stage switch port network connectivity (CSS-PNC) in a critical reliability configuration.

Enterprise survivable servers (ESS)

Note:

See *Using the Avaya Enterprise Survivable Servers (ESS)*, 03-300428, for additional information about ESS.

The Enterprise Survivable Server (ESS) is a survivability option for S8700-series and S8500/ S8500(B) systems and is available with the Communication Manger release 3.0 and later. ESS option provides survivability to an Avaya configuration by allowing backup servers to be placed in various locations in the customer's network. The backup servers (ESS servers) are given administered values that are advertised to each IPSI in the configuration. The IPSI places the ESS server on a priority list based on the administered values. If for any reason, the IPSI can no longer communicate with the Main server, the IPSI request service from the next highest priority ESS server on its list. The ESS server accepts the request and assumes control of the IPSI controlled port network.

The IPSI request for ESS service will happen after an administered "No-Service" timer expires. The value of the No-service timer determines the amount of time the IPSI will wait to request service from an ESS server, after losing communication with the Main server or the controlling ESS server. The value for the No-service timer is administrable from three to 15 minutes.

During No-Service timer interval stable calls remain up in the same state as they were before the outage occurred. The stable calls do not have access to any features such as hold, conference, etc. After the No-Service timer expires, shuffled IP to IP calls will stay up, but calls on DCP or analog phones will terminate.

When service to main is restored, the IPSI(s) will return to the control of the main server in the manner administered by the customer, which can be either manually or according to a scheduled time.

In an ESS environment, there is one Main server. The Main server can be a S8500 (B) simplex server or a pair of S8700-series servers. If the Main server is an S8500 Server, all ESS servers in the configuration must also be S8500 Servers.

ESS provides a survivability option for port networks of the following platforms:

- S8700-series fiber-PNC with ATM port network connectivity
- S8700-series fiber-PNC with CSS port network connectivity
- S8700-series/S8500(B) IP-PNC systems
- System with combination of fiber-PNC and IP-PNC

Through careful planning and consideration, S8700-series and/or S8500 Servers are placed in various locations in the customer's network. Each ESS server is administered on the Main server. The IPSIs in the configuration contain a list (called a priority list) of ESS servers. The Main server is always the highest ranking server on an IPSI's priority list.

ESS System Capacities

ESS can be administered as “local only” or as an “enterprise-wide” survivable server(s). When administered as “Local only”, which indicates it will act as the survivable server for a community or a subset of port networks, up to 63 ESS server clusters can be configured as ESS. This way the customer may configure some ESSs to serve only a few port networks in order to enable localization of failover where desired.

For enterprise-wide fail-over coverage, up to 7 ESS server clusters can be administered. The ESS which acts as a main server is called System Preferred ESS, and it must have the same capacity as the original main. For example when an S8500 Server is the System Preferred ESS to S8700/S8710 main server, it will be configured to have the same capacities as the S8700/S8710 Servers. This can be done based on its license files.

Depending on the type of failure and how the ESS servers are configured, an individual ESS server may accept control of all port networks, several port networks, a single port network, or no port networks. When a LAN or WAN failure occurs in configurations where port networks are widely dispersed, multiple ESS servers may be required to collectively accept control with each ESS server controlling some portion of the set of port networks.

When an ESS server accepts control, it communicates directly with each MCC1, CMC1, SCC1, G600, or G650 Media Gateway through the gateway’s IPSI board. In ATM PNC configuration, the ESS server can also control non-IPSI controlled port networks through an Expansion Interface board. The ESS server communicates indirectly with each G250, G350, or G700 Media Gateway through CLAN connections in the port networks.

Stable calls remain up in the same state as they were before the outage occurred. The stable calls do not have access to any features such as hold, conference, etc. The state of the stable call cannot be changed.

ESS and H.248 Media Gateways

The H.248 G700/G350/G250/G150 Media Gateways are not directly supported by the ESS feature. In the event of a failure they may re-register to ESS(s) through CLAN contained in port network which has requested an ESS, or they have the option of re-registering to an LSP.

ESS and Adjunct Survivability

Most adjuncts register with CLAN, which in the event of failure will follow the port network IPSI to an ESS. If the port network containing the CLAN cannot get service from an ESS, then the adjunct will not be survivable. Having CLAN in IPSI connected port networks will give the adjunct higher probability of survival.

Connection preserving upgrades for duplex servers

This feature is designed for preserving stable bearer connections for TDM end points and IP stations during an upgrade of S8700/S8710 duplex servers. TDM and IP connection of H.248 Media Gateways, with the S8700/S8710 being the main call controller will also be preserved.

This feature is supported on all S8700 and S8710 Linux servers running Avaya Communication Manager 3.0. It is supported on all H.248 Media Gateways and all port networks (including G650 MG). It will apply on upgrade from Avaya Communication Manager 3.0 to a newer release, and does not apply on upgrade to Avaya Communication Manager 3.0.

This feature is not call preserving and only preserves connection on stable calls. Connection preservation will not apply to calls involving H.323 IP trunks; these are H.323 IP calls and SIP calls. Connection preservation will not apply to IP trunks and ISDN-BRI stations and trunks using H.248 Media gateways resources.

Inter Gateway Alternate Routing (IGAR)

This feature enables systems with distributed branch offices and distributed call centers an alternate means of providing bearer connection between port networks and gateways when the IP-WAN is incapable of carrying the bearer traffic. IGAR may request that bearer connections be provided by the PSTN under the following conditions:

The number of calls allocated or bandwidth allocated via Call Admission Control – Bandwidth.

Limits (CAC-BL) has been reached.

- VoIP RTP resource exhaustion in a MG/PN is encountered.
- A codec set is not specified between a network region pair.
- Forced redirection between a pair of network regions is configured.
- The number of calls allocated or bandwidth allocated via Call Admission Control – Bandwidth
- Limits (CAC-BL) has been reached.

IGAR takes advantage of existing public and private-network facilities provisioned in a network region.

Most trunks in use today can be used for IGAR. Examples of the better trunk facilities for use by IGAR would be:

- Public or Private ISDN PRI/BRI
- R2MFC

IGAR is the next logical step in providing Quality of Service (QoS) to large distributed single-server configurations.

IGAR relies on Call Admission Control. When all VoIP RTP resources have been used the next attempt to get a VoIP RTP resource results in denial of the VoIP connection. Communication Manager 3.0 will attempt to use existing applications and features to redirect the call accordingly. Each IP audio stream will require a VoIP RTP resource from either a TN2302AP IP Media Processor or a G700 media gateway. Exactly how many audio streams can be supported by these resources depends on the codec selection. Upon hitting the VoIP RTP resource limit, IGAR immediately attempts to use an alternate path for a bearer connection to the network region of the called party using PSTN facilities allocated for use by the IGAR feature.

Survivability for branch office media gateways

This section describes the survivability features for branch-office media gateways.

H.248 Media Gateway recovery via LSP

If the link between the remote media gateway and the media gateway controller is broken, or the controller is down, the local survivable processor (LSP) activates and assume call processing for the media gateway. The media gateway controller can be the S8700, S8500, or S8300. The strategy by which the media gateways change control from the primary to the LSP controller is driven by the gateway using the media gateway controller list.

When the media gateway controller is an S8700-series or S8500 server

Note:

The following description applies to the S8500 as well as the S8700-series server.

In this configuration, the connectivity path between the remote Media Gateway and the S8700 Call Controller is as follows:

Media Gateway <=> IP network <=> C-LAN <=> PN back plane <=> IPSI <=> IP network <=> S8700

Link connectivity between the S8700 call controller and the G700 or G350 media gateway is monitored through the exchange of keepalive messages between the two components. If the link between the active call controller and the media gateway is severed, the gateway tries to reestablish the link using its alternate gatekeeper list. The alternate gatekeeper list is divided into primary and secondary addresses. All primary addresses receive priority weighting over the secondary addresses. Normal practice is to designate all C-LANs for the primary controller as primary gatekeeper addresses, and all the Local Survivable Processors (LSP) as secondary addresses. This practice gives a media gateway the best possible chance of registering with its primary call controller before registering with the LSP and entering into survivable mode.

In the event of a WAN failure, any IP telephone or media gateway that cannot reach the primary controlling server can register with an LSP controller in survivable mode. In the S8700/G700/G350 configuration, up to 50 LSPs are available and ready for the fail-over process. The LSP, an S8300 or S8500 Server running Avaya Communication Manager software, is always ready to acknowledge service requests from IP telephones and gateways that can no longer communicate with their main controller. Once the phones and the gateway are registered, end users at the remote site have full feature functionality. This failover process usually takes less than 5 minutes. After failover, the remote system is stable and autonomous.

S8300/G700/G350 configuration

In this configuration, the connectivity path between the G700 or G350 Media Gateway and the S8300 Server is:

Endpoint <=> IP Network <=> S8300 Server

The link failure discovery and recovery process is the same as above, except there are no C-LAN addresses in the alternate gatekeeper list. In the S8300/G700/G350 configuration, up to 10 LSPs can back up the media gateways that are controlled by the S8300 Server.

Modem dial-up backup

Modem Dial-up Backup feature provides an alternative backup path to the Enterprise headquarters, in order to maintain the control channel between the remote site and the Avaya Communication Manager in the event of main WAN failure. This feature is defined as backup interface for the primary interface for the WAN connectivity. During the switch over calls will not drop.

This feature is supported in G250, G250-BRI and in G350 H.248 Media Gateways. The dial-up back up feature and the remote router can be configured to re-establish connectivity to the main Communication Manager before the gateway or the IP phones switch over to the LSP. This feature supports dial-up to an ISP, in which case requires use of IPSec-VPN tunnel to the main site.

Auto fallback to primary Communication Manager for H.248 media gateways

This feature allows an H.248 media gateway being served by a Local Survivable Processor (LSP) to automatically return to its primary gatekeeper. This feature is connection preserving; that is, stable bearer connections will not drop during this process.

The auto fallback process

While LSP is the acting call controller, the Media Gateway attempts to register with the primary server every 30 seconds or whenever there are no active calls (this signaling also acts as keep-alive messages to the primary server). The first registration request with the primary server will set up encryption on TCP link for H.248 messages. The MG will keep LSP registration until MG is accepted by primary server. Once registered with primary, Media Gateway will drop LSP link. Once all Media Gateways have migrated form LSP, LSP will un-register all IP end points, which automatically will re-register with primary server.

This automatic migration of H.248 to primary server can be administered to happen immediately (default), or when there are no active calls, or can be scheduled for a time of a day window.

Connection preserving failover/failback for H.248 media gateways

This feature allows existing stable calls to be preserved when the media gateway fails over to another server, or LSP, or returns to its primary server. It is supported on all H.248 media gateways. It applies to failover and fallback of media gateway to or from an LSP and to or from an ESS.

During the failover/fallback process the bearer connection of stable calls are preserved. These include, analog stations and trunks, DCP stations, digital trunks, IP stations using media gateway resources, ISDN-PRI trunks, calls between gateways, IGAR, and previously connection-preserved calls.

G250 and IG550 Media Gateway standard local survivability function (SLS)

SLS is new survivable call processing engine that provides service to the media gateway when the gateway cannot reach Avaya Communication Manager. This engine is resident in the media gateway firmware and provides basic telephony functions at the branch without being registered to Avaya Communication Manager.

The SLS features are:

- Local station and outbound PSTN calling
- Inbound calls over the trunks to be delivered to available stations
- Acts as an H.323 gatekeeper for local IP phones to register (maximum of 10 IP phones can register)
- Call Detail Recording in a syslog format

During transition to survivability mode, only local IP-IP calls are preserved.

The link recovery process follows these steps:

1. While SLS is enabled and processing, the media gateway continues to seek an alternative media gateway controller.
2. If Avaya Communication Manager accepts the registration then the active IP to IP calls that shuffle are preserved.
3. The SLS application stops processing any new calls and goes to inactive mode.

IP endpoint recovery

Avaya's distributed IP-based systems can also enjoy increased availability by virtue of the "alternate gatekeeper." When IP Telephones register with Communication Manager, they are given a list of "alternate gatekeepers" to which they can re-register in the event of a failure. Thus, if a C-LAN fails or becomes unavailable, users that are registered to that C-LAN can re-home to another C-LAN that is unaffected by the failure.

IP endpoint recovery

The Avaya servers are designed to have a scalable architecture with different server components. These components provide processing and relay signaling information between Communication Manager and the Avaya IP endpoints. The system architecture is inherently distributed, providing the scalability to support a large number of endpoints and the flexibility to work in various network configurations.

This distributed nature of the architecture introduces additional complexity in dealing with endpoint recovery, since failure of any element in the end-to-end connectivity path between an IP endpoint and the switch software can result in service failure at the endpoint.

The recovery algorithm that is outlined here deals with detection and recovery from the failure of signaling channels for IP endpoints. Such failures are due to connectivity outages between the server and the endpoint, which could be due to failure in the IP network or any other component between the endpoint and the server.

In the S8500 and S8700-series configurations the connectivity path between the endpoint and the server is:

Endpoint ⇔ IP network ⇔ C-LAN ⇔ PN backplane ⇔ IPSI ⇔ IP network ⇔ S8700

In this configuration, IP endpoints register to C-LAN on the PN. The DEFINITY platforms G3r, G3si, and G3csi, which support Avaya Application Solutions features, also use C-LAN for signaling connecting to IP endpoints.

A C-LAN provides two basic reliability functions:

- A C-LAN hides server interchanges from the IP endpoints. The signaling channels of the endpoints remain intact during server interchanges, and do not have to be reestablished with the new active server.
- A C-LAN terminates TCP keepalive messages from the endpoints, and thus frees the server from handling frequent keepalive messages.

Recovery algorithm

The recovery algorithm is designed to minimize service disruption to an IP endpoint in the case of a signaling channel failure. When connectivity to a gatekeeper is lost, the IP endpoint progresses through three phases:

- Recognition of the loss of the gatekeeper
- Search for (discovery of) a new gatekeeper
- Re-registration

When the IP endpoint first registers with the C-LAN, the endpoint receives a list of alternate gatekeeper addresses from the DHCP server. The telephone uses the list of addresses to recover from a signaling link failure to the C-LAN/gatekeeper.

When the IP phone detects a failure with the signaling channel (H.225/Q.931), its recovery algorithm depends on the call state of the endpoint:

- If the user of the phone is on a call and the phone loses its call signaling channel, the new IP Robustness algorithm will allow the phone to reestablish the link with its gatekeeper without dropping the call. As a result, the call is preserved. Call features are not available during the time the phone is trying to reestablish the connection.
- If the user of the phone is not on a call, the phone closes its signaling channels and searches for a gatekeeper using the algorithm defined below.

To reestablish the link, the phone tries to register with a C-LAN on its gatekeeper list. The new C-LAN Load Balancing algorithm looks for the C-LAN on the list with the least number of phones registered to it. As a result, the recovery time will be short, and there will be no congestion due to too many phones trying to register to a single C-LAN board.

In the S8300/G700 or G350 configuration, the IP endpoint connects directly to the S8300 Server (there is no C-LAN.) The connectivity path between the endpoint and the server is:

Endpoint ⇔ IP network ⇔ S8300

To discover connectivity failure, keepalive messages are exchanged between the IP end point and the server. When the endpoint discovers that it no longer has communication with its primary gatekeeper, it looks at the next address on its list. If the next address is for an LSP, the LSP accepts the registration and begins call processing.

While the LSP is not call preserving, the fail-over from primary gatekeeper to LSP is an automatic process, and does not require human intervention. The fail-back from LSP to primary gatekeeper, however, is not currently automatic, and requires a system reset on the LSP. During the fail-back to the primary gatekeeper, all calls are dropped, with the exception of IP-to-IP calls.

IP Endpoint Time to Service

The Time to Service (TTS) feature improves the time required to bring an IP phone system into service by reducing the amount of required signaling for a phone to reach the in-service state. Once a phone is registered, TTS keeps the registration persistent for a relatively long Time to Live (hours) regardless of TCP connection failure, network outages, or even restarts of the endpoint. This significantly reduces the number of times that IP phones need to re-register with Communication Manager due to outages. As a result, the TTS feature improves system availability after a network outage.

There are two functions in TTS that improve IP endpoints availability. One function is that the IP Endpoint Time-To-Service feature changes the way IP endpoints register with their gatekeeper, reducing the time to come into service. In the current Avaya Communication Manager architecture, there are two activities to bring the IP endpoints into service. The H.323 IP endpoint must register with the communication manager and then it must establish a TCP socket connection between the server and the endpoint for call signaling. Since all the IP endpoints in a system strive to get into service as quickly as possible after an outage, the main processor can be flooded with activity. In a system with a large number of IP endpoints, this flooding leads to delays not only for phones trying to get into service, but also for endpoints already in service trying to make calls.

With Avaya Communication Manager Release 4.0, the TTS separates the timing of the H.323 registration process from the timing of the TCP socket-connection setup process. This decoupling of the steps considerably improves the time for phones to be in-service.

With TTS, after all the IP phones within a system register to the Communication Manager, the TCP socket is established when the processor occupancy level returns to normal. However, when the main processor occupancy level is high, the TCP socket is established on demand (when users make a first call or when a call needs to be delivered to a user) or via background maintenance. Once the TCP socket is established, the socket remains up for subsequent calls. In addition, with TTS, Communication Manager, rather than the IP endpoint, initiates the establishment of the TCP socket resulting in faster establishment of TCP sockets.

The second function of TTS significantly reduce the number of times that IP endpoints need to re-register with the Communication Manager. This feature provides the capability to persist IP endpoint registrations across many network failures and other outages. Currently, whenever TCP sockets are dropped, the IP endpoints must re-register. With TTS, IP endpoints will not usually need to re-register for network outages that do not cause the system to failover to an Enterprise Survivable Server (ESS) or Local Survivable Processor (LSP). Since most issues with registration delays in the past have been after short network outages, this capability dramatically reduces the number of times that an IP endpoint needs to re-register with Communication Manager.

If re-registration is not required, only the re-establishment of the TCP socket is needed, which is also done in an on-demand fashion. Currently, in a call center environment, the agents must always log-in again whenever the endpoint becomes un-registered. As a consequence of not requiring re-registrations after most outages, the agents' log-ins persist and they do not need to log-in again.

Note that re-registration is still required for outages that cause the IP endpoints to failover to an ESS or LSP (and then again when they recover back to the original server). In addition, a Communication Manager reset of level 2 (or higher) or a power cycle on the IP endpoints also requires IP endpoints to re-register because the information for the registration is erased under these conditions. For security reasons, IP endpoints also need to re-register with Communication Manager if they have not been able to communicate with Communication Manager over the RAS signaling channel for an extended period of time.

Changes in IP end points

TTS features work only if corresponding changes are made to the Avaya H.323-based IP endpoints. The TTS algorithms are implemented in the IP endpoints, starting with IP Telephone R3.1, Softphone R6, and post-R5.2 IP Agent releases. These TTS-enabled endpoints continue to support previous link recovery algorithms when communicating with a server that does not support TTS or does not have TTS enabled.

The TTS features works seamlessly with older IP endpoints. However, the benefits of the features are limited to the number of TTS-capable endpoints deployed with Communication Manager 4.0 and beyond.

Operation with NAT/Firewall Environment

With TTS algorithm, the TCP connection for call signaling channel is initiated by the server, not by the endpoints, as was done prior to TTS. With server-based NAT or firewall environments, the firewalls must be configured appropriately to allow TCP connections from the server to the endpoints. These firewall rules are the reverse, in terms of direction, of the firewall rules prior to the TTS algorithm.

Converged Network Analyzer for network optimization

The Converged Network Analyzer (CNA) is an offer from the Application Assurance Networking line of products from Avaya. In conjunction with a network design that provides multiple diverse paths, the CNA path optimization feature can be used to significantly enhance the reliability of the voice communication system.

CNA can alleviate the effect of WAN problems on voice communication by ensuring that traffic is always sent on the path that is experiencing the least amount of network related problems. In the event of a network problem on a path that's currently in use by the voice communication system, CNA intervenes in real time to move the traffic to a path that experiences no such problems.

This path optimization feature can be used to protect both the voice bearer traffic and the voice signaling traffic. Studies have shown that enabling CNA path optimization can yield more than an order of magnitude improvement in application availability. See Section 3: Getting the IP network ready for telephony for more information on CNA.

Section 3: Getting the IP network ready for telephony

IP Telephony network engineering overview

In the early days of local area networking, network designers used hubs to attach servers and workstations, and routers to segment the network into manageable pieces. Because of the high cost of router interfaces and the inherent limitations of shared-media hubs, network design was generally well done. In recent years, with the rise of switches to segment networks, designers were able to hide certain faults in their networks and still get good performance. As a result, network design was often less than optimal. IP Telephony places new demands on the network. Suboptimal design cannot cope with these demands. Even with switches installed, a company must follow industry best practices to have a properly functioning voice network. Because most users do not tolerate poor voice quality, administrators should implement a well-designed network before they begin IP Telephony pilot programs or deployments.

This section contains network design recommendations in the following topics:

Overview

Industry best practices dictate that a network be designed with consideration of the following factors:

- Reliability and redundancy
- Scalability
- Manageability
- Bandwidth

Voice mandates consideration of the following additional factors when designing a network:

- Delay
- Jitter
- Loss
- Duplex

In general, these concerns dictate a hierarchical network that consists of at most three layers (Table 48: Layers in a hierarchical network on page 284):

- Core
- Distribution
- Access

Some smaller networks can collapse the functions of several layers into one device.

Table 48: Layers in a hierarchical network

Layer	Description
Core	The core layer is the heart of the network. The purpose of the core layer is to forward packets as quickly as possible. The core layer must be designed with high availability in mind. Generally, these high-availability features include redundant devices, redundant power supplies, redundant processors, and redundant links. Today, core interconnections increasingly use Gigabit Ethernet or 10 Gigabit Ethernet.
Distribution	The distribution layer links the access layer with the core. The distribution layer is where QoS feature and access lists are applied. Generally, Gigabit Ethernet connects to the core, and either Gigabit Ethernet or 100base-TX/FX links connect the access layer. Redundancy is important at this layer, but not as important as in the core. This layer is combined with the core in smaller networks.
Access	The access layer connects servers and workstations. Switches at this layer are smaller, usually 24 to 48 ports. Desktop computers, workstations, and servers are usually connected at 100 Mbps or 1 Gbps. Limited redundancy is used. Some QoS and security features can be implemented in the access layer. Power over Ethernet (PoE) is included to power IP telephones and other access devices.

For IP Telephony to work well, WAN links must be properly sized with sufficient bandwidth for voice and data traffic. Each voice call uses 9.6 Kbps to 120 Kbps, depending on the desired codec, payload size, and header compression used. Additional bandwidth might be used if wideband audio or video is implemented. The G.729 compression algorithm, which uses about 27 Kbps of bandwidth, is one of the most used standards today. Traditional telephone metrics, such as average call volume, peak volume, and average call length, can be used to size interoffice bandwidth demands. See Traffic engineering for more information.

Quality of Service (QoS) also becomes increasingly important with WAN circuits. In this case, QoS means the classification and the prioritization of voice traffic. Voice traffic must be given absolute priority through the WAN. If links are not properly sized or queuing strategies are not properly implemented, the quality and the timeliness of voice and data traffic will be less than optimal.

The following WAN technologies are commonly used with IP Telephony:

- MPLS (Multiprotocol Label Switching)
- ATM (Asynchronous Transfer Mode)
- Frame Relay
- Point-to-point (PPP) circuits
- Internet VPNs

The first four technologies all have good throughput, low latency, and low jitter. MPLS and ATM have the added benefit of enhanced QoS. MPLS is a relatively new service offering and currently has issues with momentary outages of 1 to 50 seconds duration. The Avaya Converged Network Analyzer product can be used to improve MPLS performance.

Frame Relay WAN circuits can be difficult to use with IP Telephony. Congestion in Frame Relay networks can cause frame loss, which can significantly degrade the quality of IP Telephony conversations. With Frame Relay, proper sizing of the committed information rate (CIR) is critical. In a Frame Relay network, any traffic that exceeds the CIR is marked as discard eligible, and is discarded at the option of the carrier if it experiences congestion in its network. Because voice packets must not be dropped, CIR must be sized to maximum traffic usage. Also, Service Level Agreements (SLAs) must be established with the carrier to define maximum levels of delay and frame loss, and remediation if the agreed-to levels are not met.

Internet VPNs are economical but more prone to quality issues than the other four technologies.

Network management is another important area to consider when implementing IP Telephony. Because of the requirements imposed by IP Telephony, it is critical to have an end-to-end view of the network, and ways to implement QoS policies globally. Products such as HP OpenView Network Node Manager, Avaya Integrated Management, Avaya Converged Network Analyzer (CNA), Concord NetHealth, and MRTG help administrators maintain acceptable service. Outsource companies are also available to assist other companies that do not have the resources to implement and maintain network management.

Voice quality

Voice quality is always a subjective topic. Defining “good” voice quality varies with business needs, cultural differences, customer expectations, and hardware and software. The requirements set forth are based on the ITU-T and EIA/TIA guidelines and extensive testing at Avaya Labs. Avaya requirements meet or exceed most customer expectations. However, the final determination of acceptable voice quality lies with the customer’s definition of quality, and the design, implementation, and monitoring of the end-to-end data network.

Quality is not one discrete value where the low side is good and the high side is bad. A trade-off exists between real-world limits and acceptable voice quality. Lower delay, jitter, and packet loss values can produce the best voice quality, but also can come with a cost to upgrade the network infrastructure to get to the low values. Another real-world limit is the inherent WAN delay. An IP

trunk that links the west coast of the United States to India could add a fixed delay of 150 milliseconds (ms) into the overall delay budget.

Perfectly acceptable voice quality is attainable, but will not be “toll” quality. Therefore, Avaya presents a tiered choice of elements that make up the requirements.

The critical objective factors in assessing IP Telephony quality are delay, jitter, and packet loss. To ensure good and consistent levels of voice quality, Table 49: Factors that affect voice quality on page 286 lists Avaya’s suggested network requirements. These requirements are true for both LAN only and for LAN and WAN connections.

Table 49: Factors that affect voice quality

Network factor	Measurement[1]
Delay (one-way between endpoints)	• A delay of 80 ms or less can, but may not, yield the best quality. • A delay of 80 ms to 180 ms can yield business-communication quality. Business-communication quality is much better than cell-phone quality, and is well-suited for the majority of businesses.[2] • Delays that exceed 180 ms might still be quite acceptable depending on customer expectations, analog trunks used, codec type, and so on.
Jitter (variability of the delay between endpoints)	• 20 ms, or less than half the sample size, for the best quality. **Note:** This value has some latitude, depending on the type of service that the jitter buffer has in relationship to other router buffers, the packet size used, and so on.
Packet loss (maximum packet/ frame loss between endpoints)	• <1% can yield the best quality, depending on many factors. • <3% should give business-communications quality, which is much better than cell-phone quality.[2] • >3% might be acceptable for voice, but might interfere with signaling.

1. All measurement values are between endpoints because this document assumes that IP Telephony is not yet implemented. All values therefore reflect the performance of the network without endpoint consideration.
2. Also, “business-communication quality” is defined as less than toll quality, but much better than cell-phone quality.

For more information see Voice quality network requirements.

The Converged Network Analyzer (CNA) can help you measure and report on network delay, jitter, and packet loss. CNA can also provide you with a rating of voice quality using the 0-5 APR score (see CNA Application Performance Rating on page 254).

With the optional Path Optimization feature, CNA can also help you optimize voice performance, hence insure that voice quality is acceptable. For more information on CNA see The Converged Network Analyzer on page 344.

Best practices

To consistently ensure the highest quality voice, Avaya highly recommends consideration of the following industry best practices when implementing IP Telephony. Note that these suggestions are options, and might not fit individual business needs in all cases.

- **QoS/CoS**. QoS for voice packets is obtained only after a Class of Service (CoS) mechanism tags voice packets as having priority over data packets. Networks with periods of congestion can still provide excellent voice quality when using a QoS/CoS policy. The recommendation for switched networks is to use IEEE 802.1p/Q. The recommendation for routed networks is to use DiffServ Code Points (DSCP). The recommendation for mixed networks is to use both. Port priority can also be used to enhance DiffServ and IEEE 802.1p/Q. Even networks with plentiful bandwidth should implement CoS/QoS to protect voice communications from periods of unusual congestion, such as a computer virus might cause.
- **Switched network**. A fully switched LAN network is a network that allows full duplex and full endpoint bandwidth for every endpoint that exists on that LAN. Although IP Telephony systems can work in a shared or hub-based LAN, Avaya recommends the consistently high results that a switched network lends to IP Telephony.
- **Network assessment**. A Basic Network Readiness Assessment Offer from Avaya is vital to a successful implementation of IP Telephony products and solutions. Contact an Avaya representative or authorized dealer to review or certify your network. Network assessment offer explains the options that are available with this offer.
- **VLANs**. Placing voice packets on a separate VLAN or subnetwork from data packets is a generally accepted practice to reduce broadcast traffic and to reduce contention for the same bandwidth as voice. Note that Avaya IP Telephones provide excellent broadcast storm protection. Other benefits become available when using VLANs, but there can be a substantial cost with initial administration and maintenance. VLANs on page 291 explains this concept further.

Common issues

Some common negative practices that can severely impact network performance, especially when using IP Telephony, include:

- **A flat, non-hierarchical network**, for example, cascading small workgroup switches together. This technique quickly results in bottlenecks, because all traffic must flow across the uplinks at a maximum of 10 Gbps, versus traversing switch fabric at speeds of 256 Gbps or greater. The greater the number of small switches or layers, the greater the number of uplinks, and the lower the bandwidth for an individual connection. Under a network of this type, voice performance can quickly degrade to an unacceptable level.
- **Multiple subnets on a VLAN**. A network of this type can have issues with broadcasts, multicasts, and routing protocol updates. This practice can have a significant negative impact on voice performance, and complicate troubleshooting.
- **A hub-based network**. Hubs in a network create some interesting challenges for administrators. It is advisable not to link more than four 10baseT hubs or two 100baseT hubs together. Also, the *collision domain*, the number of ports that are connected by hubs without a switch or router in between, should be kept as low as possible. Finally, the effective (half-duplex) bandwidth that is available on a shared collision domain is approximately 35% of the total bandwidth that is available.
- **Too many access lists**. Access lists slow down a router. While access lists are appropriate for voice networks, care must be taken not to apply them to unnecessary interfaces. Traffic should be modeled beforehand, and access lists applied only to the appropriate interface in the appropriate direction, not to all interfaces in all directions.

Avaya recommends caution when using the following:

- **Network Address Translation (NAT)**. IP Telephony may not work across Network Address Translation (NAT), because if private IP addresses are exchanged in signaling messages, these addresses are not reachable from the public side of the NAT and cannot be used for the media sessions. See NAT on page 302 for more information on the problem and solutions for using NAT with IP Telephony.
- **Analog dial-up**. Be careful in using analog dial-up (56 K) to connect two locations. Upstream bandwidth is limited to a maximum of 33.6 K, and in most cases is less. This results in insufficient bandwidth to provide toll-quality voice. Some codecs and network parameters provide connections that are acceptable, but consider each connection individually.
- **Virtual Private Network (VPN)**. Large delays are inherent in some VPN software products due to encryption, decryption, and additional encapsulation. Some hardware-based products, including Avaya VPN products, encrypt at near wire speed, and can be used. In addition, if the VPN is run over the Internet, sufficient quality for voice cannot be guaranteed unless delay, jitter, and packet loss are contained within the parameters that are listed above. See VPN for more information.

Network design

This section discusses the network design process for IP Telephony. This section focuses on:

- LAN issues
- WAN
- VPN
- NAT

LAN issues

This section covers Local Area Network (LAN) issues, including speed and duplex, inline power, hubs versus switches, and so on:

General guidelines

Because of the time-sensitive nature of IP Telephony applications, IP Telephony should be implemented on an entirely switched network. Ethernet collisions, which are a major contributor to delay and jitter, are virtually eliminated on switched networks. Additionally, the C-LAN, Media Processor board, and IP Telephones should be placed on a separate subnetwork or VLAN (that is, separated from other non-IP Telephony hosts). This separation provides for a cleaner design where IP Telephony hosts are not subjected to broadcasts from other hosts, and where troubleshooting is simplified. This separation also provides a routed boundary between the IP Telephony segments and the rest of the enterprise network, where restrictions can be placed to prevent unwanted traffic from crossing the boundary. When personal computers are attached to IP Telephones, the uplink to the Ethernet switch should be a 100 Mbps link or greater, so that there is more bandwidth to be shared between the telephone and the computer.

Sometimes enterprises are unable to follow these guidelines, and Avaya's solutions can be made to work in some less-than-ideal circumstances. If IP Telephones will share a subnetwork with other hosts, the IP Telephones should be placed on a subnetwork of manageable size (24-bit subnet mask or larger, with 254 hosts or less), with as low a rate of broadcasts as possible. If the broadcast level is high, remember that 100-Mbps links are less likely to be overwhelmed by broadcast traffic than 10-Mbps links. Perhaps a worst-case example is the scenario where Avaya IP Telephones are deployed on a large subnetwork that is running IPX or other broadcast-intensive protocol, with broadcasts approaching 500 per second. Although the performance of the IP Telephones and the voice quality can be satisfactory in this environment, this type of deployment is strongly discouraged.

Ethernet switches

The following recommendations apply to Ethernet switches to optimize operation with Avaya endpoints. Theses recommendations are meant to provide the simplest configuration by removing unnecessary features.

- Enable spanning tree fast start feature or disable spanning tree at the port level. The Spanning Tree Protocol (STP) is a Layer 2 loop-avoidance protocol. When a device is first connected (or reconnected) to a port that is running spanning tree, the port takes approximately 50 seconds to cycle through the Listening, Learning, and Forwarding states. This 50-second delay is neither necessary nor desired on ports that are connected to IP endpoints. Instead, enable a fast start feature on these ports to put them into the Forwarding state almost immediately. If this feature is not available, disabling spanning tree on the port is an option that should be considered. Do not disable spanning tree on an entire switch or VLAN. Also, Rapid Spanning Tree Protocol (802.1w) is always preferred over STP (802.1D).
- Disable Cisco features. Cisco features that are not required by Avaya endpoints include channeling, cdp, and proprietary (not 802.3af) inline power. These features are nonstandard mechanisms that are relevant only to Cisco devices, and can sometimes interfere with Avaya devices. The CatOS command **`set port host <mod/port>`** automatically disables channeling and trunking, and enables portfast. Execute this command first, and then manually disable cdp and Cisco proprietary (not 802.3af) inline power. Then manually enable 802.1Q trunking as necessary.
- Properly configure 802.1Q trunking on Cisco switches. When trunking is required on a Cisco CatOS switch that is connected to an Avaya IP Telephone, enable it for 802.1Q encapsulation in the no-negotiate mode (**`set trunk <mod/port> nonegotiate dot1q`**). This causes the port to become a plain 802.1Q trunk port with no Cisco autonegotiation features. When trunking is not required, explicitly disable it, because the default is to autonegotiate trunking.

Speed and duplex

One major issue with Ethernet connectivity is proper configuration of speed and duplex. A significant amount of misunderstanding exists in the industry as a whole with regard to the auto-negotiation standard. It is imperative that the speed and duplex settings be configured properly.

A duplex mismatch condition results in a state where one side perceives a high number of collisions, while the other side does not. This results in packet loss. Although it degrades performance in all cases, this level of packet loss might go unnoticed in a data network because protocols such as TCP retransmit lost packets. In voice networks, however, this level of packet loss is unacceptable. Voice quality rapidly degrades in one direction. When voice quality problems are experienced, duplex mismatches are the first thing to investigate.

In general, best practice is to lock down both sides of an IP connection to 100 Mbps and full duplex. However, auto-negotiate is an acceptable practice in most circumstances.

VLANs

Virtual Local Area Networks (VLANs) are an often-misunderstood concept. This section begins by defining VLANs, and then addresses configurations that require the Avaya IP Telephone to connect to an Ethernet switch port that is configured for multiple VLANs. The IP Telephone is on one VLAN, and a personal computer that is connected to the telephone is on a separate VLAN. Three sets of configurations are given: Avaya C360, Cisco CatOS, and some Cisco IOS.

VLAN defined

With simple Ethernet switches, the entire switch is one Layer 2 broadcast domain that usually contains one IP subnetwork (Layer 3 broadcast domain). Think of a single VLAN (on a VLAN-capable Ethernet switch) as being equivalent to a simple Ethernet switch. A VLAN is a logical Layer 2 broadcast domain that typically contains one IP subnetwork. Therefore, multiple VLANs contain logically separated subnetworks. This arrangement is analogous to multiple switches being physically separated subnetworks. A Layer 3 routing process is required to route between VLANs, just as one is required to route between subnetworks. This routing process can take place on a connected router or a router module within a Layer 2/Layer 3 Ethernet switch. If no routing process is associated with a VLAN, devices on that VLAN can only communicate with other devices on the same VLAN.

The port or native VLAN

Port VLAN and native VLAN are synonymous terms. The IEEE 802.1Q standard and most Avaya switches use the term *port VLAN*, but Cisco switches use the term *native VLAN*. Issue the **show trunk** command on C360s and CatOS Catalysts to see which term is used in the display output.

Every port has a port VLAN or a native VLAN. Unless otherwise configured, it is VLAN 1 by default. It can be configured on a per-port basis with the commands in Table 50.

Table 50: Commands to configure a port VLAN or a native VLAN

Avaya C360	Cisco CatOS
set port vlan <id> <mod/port>	**set vlan <id> <mod/port>**

All untagged Ethernet frames (with no 802.1Q tag, for example, from a personal computer) are forwarded on the port VLAN or the native VLAN. This is true even if the Ethernet switch port is configured as an 802.1Q trunk, or otherwise configured for multiple VLANs. For more information, see VLAN binding feature (C360).

Trunk configuration

A trunk port on an Ethernet switch is one that is capable of forwarding Ethernet frames on multiple VLANs through the mechanism of VLAN tagging. IEEE 802.1Q specifies the standard method for VLAN tagging. Cisco also uses a proprietary method called ISL. Avaya products do not interoperate with ISL.

A trunk link is a connection between two devices across trunk ports. This connection can be between a router and a switch, between two switches, or between a switch and an IP Telephone. Some form of trunking or forwarding multiple VLANs must be enabled to permit the IP Telephone and the attached personal computer to appear on separate VLANs. The commands in Table 51 enable trunking.

Table 51: Administration commands for VLAN trunking

Avaya C360	Cisco CatOS
set trunk <mod/port> dot1q By default, all VLANs (1 to 3071) are enabled on the trunk port. VLANs can be specified using VLAN binding commands.	**set trunk <mod/port> nonegotiate dot1q** By default, all VLANs (1 to1005) are enabled on the trunk port. VLANs can be selectively removed with the command **clear trunk <mod/port> <vid>**.

Note that Cisco and Avaya can remove VLANs from a trunk port. This is a highly desirable feature because only two VLANs at most should appear on a trunk port that is connected to an IP Telephone. That is, broadcasts from nonessential VLANs should not be permitted to bog down the link to the IP Telephone.

VLAN binding feature (C360)

The default behavior of trunking is to permit all VLANs. In addition, the port does not need to be a trunk at all to forward multiple VLANs.

To enable VLAN binding:

1. Verify that the port is configured with the desired port VLAN or native VLAN.
2. Add additional VLANs with one of the following VLAN-binding-mode options:

   Static option

   a. Put the port in bind-to-static mode by typing **set port vlan-binding-mode <mod/port> static**.

   b. Statically add another VLAN in addition to the port VLAN or the native VLAN by typing **set port static-vlan <mod/port> <vid>**.

   Configured option

   c. Add a VLAN to the configured VLAN list by typing **set vlan <id>**.

   d. Type **show vlan** to see entire list.

e. Apply the configured VLANs to the port, and permit only those VLANs (bind-to-all permits all VLANs and not just the configured) by typing **set port vlan-binding-mode <mod/port> bind-to-configured**

3. For simplicity, Avaya recommends using the static option for IP Telephony. If the port is connected to a router or to another switch, trunking must be enabled with the command **set trunk <mod/port> dot1q**, which causes all egress frames to be tagged. However, if the port is connected to an Avaya IP Telephone with an attached personal computer, trunking must not be enabled so that none of the egress frames are tagged. This is necessary because most personal computers cannot understand tagged frames.

Setting the priority without trunking or VLAN binding (single-VLAN scenario)

With Avaya, it is possible to set the Layer 2 priority on the IP Telephone, even if the telephone is not connected to a trunk or multi-VLAN port. That is, the Avaya switch does not need to be explicitly configured to accept priority-tagged Ethernet frames on a port with only the port VLAN or the native VLAN configured. This is useful if the telephone and the attached personal computer are on the same VLAN (same IP subnetwork), but the telephone traffic requires higher priority. Enable 802.1Q tagging on the IP phone, set the priorities as desired, and set the VID to zero. Per the IEEE standard, a VID of zero assigns the Ethernet frame to the port VLAN or the native VLAN.

Cisco switches behave differently in this scenario, depending on the hardware platforms and OS versions.

Note:

Setting a Layer 2 priority is useful only if QoS is enabled on the Ethernet switch. Otherwise, the priority-tagged frames are treated no differently than clear frames.

WAN

Because of the high costs and lower bandwidths available, there are some fundamental differences in running IP Telephony over a Wide Area Network (WAN) versus a LAN. Because of the resource scarcity, it is important to consider network optimizations and proper network design, because problems are more likely to manifest themselves in a WAN environment.

Topics covered include:

- Overview
- Frame Relay
- MPLS

Overview

QoS

In particular, Quality of Service (QoS) becomes more important in a WAN environment than in a LAN. In many cases, transitioning from the LAN to the WAN reduces bandwidth by approximately 99%. Because of this severe bandwidth crunch, strong queuing, buffering, and packet loss management techniques have been developed. These are covered in more detail in the Quality of Service guidelines chapter.

Recommendations for QoS

For many customers, including small and medium, simplicity is more effective than complex configurations when implementing QoS for voice, data, signaling and video. If traffic engineering is done properly and sufficient bandwidth is available, especially for WAN links, voice and voice signaling traffic can both be tagged as DSCP 46. This Class of Service (CoS) tagging will place both types of packets into the same High Priority queue with a minimum of effort. The key is to have enough bandwidth to prevent any packets from dropping.

For large enterprises and Multi-National companies, a stratified approach to CoS makes sense. This allows maximum control for many data and voice services. For this environment, Avaya recommends using DSCP 46 (Expedited Forwarding) for voice (bearer), but voice signaling and especially IPSI signaling could have their own DSCP values and dedicated bandwidth. This would prevent traffic, like voice bearer from contending with signaling. Although the configuration may be more complex to manage and administer, the granularity will give the best results and is recommended as a best practice.

At the routers, Avaya recommends using strict priority queuing for voice packets, and weighted-fair queuing for data packets. Voice packets should always get priority over non-network-control data packets. This type of queuing is called Class-Based Queuing (CBQ) on Avaya data networking products, or Low-Latency Queuing (LLQ) on Cisco routers.

Codec selection and compression

Because of the limited bandwidth that is available on the WAN, using a compressed codec allows much more efficient use of resources without a significant decrease in voice quality. Avaya recommends that IP Telephony implementations across a WAN use the G.729 codec with 20-ms packets. This configuration uses 24 Kbps (excluding Layer 2 overhead), 30% of the bandwidth of the G.711 uncompressed codec (80 Kbps). For more information on bandwidth, see IP bandwidth and Call Admission Control on page 216.

To conserve even more bandwidth, RTP header compression (cRTP) can be used on point-to-point links. cRTP reduces the IP/UDP/RTP overhead from 40 bytes to 4 bytes. With 20-ms packets, this translates to a savings of 14.4 Kbps, making the total bandwidth required for G.729 approximately 9.6 Kbps. The trade-off for cRTP is higher CPU utilization on the router. The processing power of the router determines the amount of compressed RTP traffic that the router can handle. Avaya testing indicates that a typical small branch-office router can handle 768 Kbps of compressed traffic. Larger routers can handle greater amounts. cRTP is available on Avaya, Extreme, Juniper, and Cisco routers.

Serialization delay

Serialization delay refers to the delay that is associated with sending bits across a physical medium. Serialization delay is important to IP Telephony because this delay can add significant jitter to voice packets, and thus impair voice quality. See Layer 3 QoS on page 317 for techniques to minimize serialization delay.

Network design

Routing protocols and convergence

When designing a IP Telephony network across a WAN, some care should be taken when selecting a routing protocol or a dial-backup solution. Different routing protocols have different convergence times, which is the time that it takes to detect a failure and route around it. While a network is in the process of converging, all voice traffic is lost.

The selection of a routing protocol depends on several factors:

- If a network has a single path to other networks, static routes are sufficient.
- If multiple paths exist, is convergence time an issue? If so, EIGRP and OSPF are appropriate.
- Are open standards-based protocols required? If so, OSPF and RIP are appropriate, but not EIGRP or IGRP, which are Cisco proprietary.

In general, Avaya recommends the use of OSPF when routing protocols are required. OSPF allows for relatively fast convergence, and does not rely on proprietary protocols.

In many organizations, because of the expense of dedicated WAN circuits, dial-on-demand circuits are provisioned as backup if the primary link fails. The two principal technologies are ISDN (BRI) and analog modem. ISDN dial-up takes approximately 2 seconds to connect, and offers 64 Kbps to 128 Kbps of bandwidth. Analog modems take 60 seconds to connect, and offer up to 56 Kbps of bandwidth. If G.729 is used as the codec, either technology can support IP Telephony traffic. If G.711 is used as the codec, only ISDN is appropriate. Also, because of the difference in connect times, ISDN is the preferred dial-on-demand technology for implementing IP Telephony.

Multipath routing

Many routing protocols, such as OSPF, install multiple routes for a particular destination into a routing table. Many routers attempt to load-balance across the two paths. There are two methods for load balancing across multiple paths. The first method is per-packet load balancing, where each packet is serviced round-robin fashion across the two links. The second method is per-flow load balancing, where all packets in an identified “flow” (source and destination addresses and ports) take the same path. IP Telephony does not operate well over per-packet load-balanced paths. This type of setup often leads to “choppy” quality voice. Avaya recommends that in situations with multiple active paths, per-flow load balancing is preferable to per-packet load balancing. This behavior is enabled by default on Avaya products. On Cisco routers, the command for this is “ip route-cache,” applied per interface.

Frame Relay

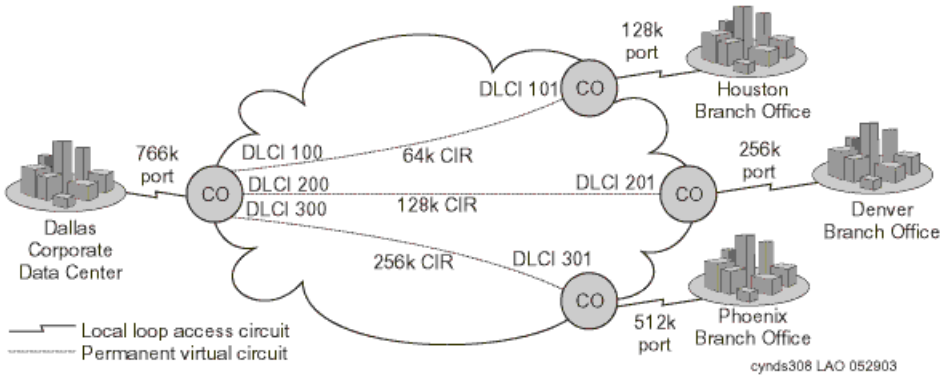
The nature of Frame Relay poses somewhat of a challenge for IP Telephony, as described in this section.

Overview of frame relay

Frame Relay service is composed of three elements: the physical access circuit, the Frame, Relay port, and the virtual circuit. The physical access circuit is usually a T1 or fractional T1 and is provided by the local exchange carrier (LEC) between the customer premise and the nearest central office (CO). The Frame Relay port is the physical access into the Frame Relay network, a port on the Frame Relay switch itself.

The access circuit rate and the Frame Relay port rate must match. The virtual circuit is a logical connection between Frame Relay ports that can be provided by the LEC for intra-lata Frame Relay, or by the inter-exchange carrier (IXC) for inter-lata Frame Relay. The most common virtual circuit is a permanent virtual circuit (PVC), which is associated with a committed information rate (CIR). The PVC is identified at each end by a separate data-link connection identifier (DLCI) in Figure 79.

Figure 79: Data-link connection identifiers over an interexchange carrier Frame Relay network



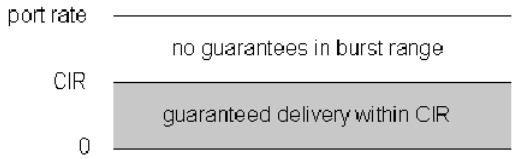
This hypothetical implementation shows the Dallas corporate office connected to three branch offices in a common star topology (or hub and spoke). Each office connects to a LEC CO over a fractional T1 circuit, which terminates onto a Frame Relay port at the CO, and onto a Frame Relay capable router at the customer premise. The port rates and the access circuit rates match. PVCs are provisioned within the Frame Relay network between Dallas and each branch office. The CIR of each PVC is sized so that it is half the respective port rate, which is a common implementation. Each branch office is guaranteed its respective CIR, but it is also allowed to burst up to the port rate without any guarantees.

The port rate at Dallas is not quite double the aggregate CIR, but it does not need to be, because the expectation is that not all three branch offices will burst up to the maximum at the same time. In an implementation like this, the service is probably negotiated through a single vendor. But it is likely that Dallas and Houston are serviced by the same LEC, and that the Frame Relay is intra-lata, even if it was negotiated through an IXC, such as AT&T, WorldCom, or Sprint. The service between Dallas and the other two branch offices, however, is most likely inter-lata.

A frame relay issue and alternatives

The obstacle in running IP Telephony over Frame Relay involves the treatment of traffic within the CIR and outside of CIR, commonly termed the “burst range.”

Figure 80: Committed information rate (burst range)



As Figure 80: Committed information rate (burst range) shows, traffic up to the CIR is guaranteed, whereas traffic beyond the CIR usually is not. This is how Frame Relay is intended to work. CIR is a committed and reliable rate, whereas burst is a bonus when network conditions permit it without infringing upon the CIR of any user. For this reason, burst frames are marked as discard eligible (DE), and are queued or discarded when network congestion exists. Although experience has shown that customers can achieve significant burst throughput, it is unreliable and unpredictable, and not suitable for real-time applications like IP Telephony.

Therefore, the objective is to prevent voice traffic from entering the burst range and being marked DE. One way to accomplish this is to prohibit bursting by shaping the traffic to the CIR and setting the excess burst size (B_e – determines the burst range) to zero. However, this also prevents data traffic from using the burst range.

Additional frame relay information

One interesting piece of knowledge is that most IXCs convert the long-haul delivery of Frame Relay into ATM. That is, the Frame Relay PVC is converted to an ATM PVC at the first Frame Relay switch after leaving the customer premise. It is not converted back to Frame Relay until the last Frame Relay switch before entering the customer premise. This is significant because ATM has built- in Class of Service (CoS). A customer can contract with a carrier to convert the Frame Relay PVC into a constant bit rate (CBR) ATM PVC. ATM CBR cells are delivered with lower latency and higher reliability.

Finally, under the best circumstances, Frame Relay is still inherently more susceptible to delay than ATM or TDM. Therefore, after applying the best possible queuing mechanism, one should still expect more delay over Frame Relay than is present over ATM or TDM.

MPLS

MultiProtocol Label Switching (MPLS) VPN service from service providers is commonly used by enterprises for WAN connectivity. The service is often available over different types of access links, and usually offers multiple classes of service. MPLS service is typically expected to provide good QoS and therefore to satisfy VoIP requirements, though this often depends on the Service Layer Agreement (SLA) and the actual quality delivered by the service provider.

With MPLS service, unlike private WAN, the enterprise controls QoS explicitly only on the access link —- that is, on the connection from each enterprise site to the MPLS network. Within the MPLS network QoS is controlled by the service provider. The enterprise affects the service given to its traffic by assigning the traffic to appropriate classes of service in the service provider’s network. This is done with DiffServ Code Point (DSCP) marking in the packet’s IP header. DSCP remarking by the enterprise edge routers may be required, mapping the DSCPs of enterprise traffic to the DSCP values designated by the MPLS service provider for the different classes of service in their service offering.

VPN

Many definitions exist for Virtual Private Networks (VPNs). VPNs refer to encrypted tunnels that carry packetized data between remote sites. VPNs can use private lines, or use the Internet through one or more Internet Service Providers (ISPs). VPNs are implemented in both dedicated hardware and software, but can also be integrated as an application to existing hardware and software packages. A common example of an integrated package is a firewall product that can provide a barrier against unauthorized intrusion, as well as perform the security features that are needed for a VPN session.

The encryption process can take from less than 1 millisecond (ms) to 1 second or more, at each end. Obviously, VPNs can represent a significant source of delay, and therefore have a negative affect on voice performance. Avaya VPN products encrypt traffic with less than 1ms of delay, and thus are appropriate for IP Telephony. Also, because most VPN traffic runs over the Internet and there is little control over QoS parameters for traffic crossing the Internet, voice quality may suffer due to excessive packet loss, delay, and jitter. Users might be able to negotiate a service-level agreement with the VPN provider to guarantee an acceptable level of service. Before implementing IP Telephony with a VPN, users should test their VPN network over time to ensure that it consistently meets the requirements that are specified in the *Avaya IP Voice Quality Network Requirements Document Summary*.

Convergence advantages

For increasing numbers of enterprises, the VPN carries not only data, but voice communications. Though voice communication over IP networks (IP Telephony) creates new quality of service (QoS) and other challenges for network managers, there are compelling reasons for moving forward with convergence over maintaining a traditional voice and data infrastructure:

- A converged infrastructure makes it easier to deploy eBusiness applications, such as customer care applications, that integrate voice, data, and video.
- Enterprises can reduce network costs by combining disparate network infrastructures, and eliminating duplicate facilities.
- A converged infrastructure can increase the efficiencies of the IT organization.
- Long distance charges can be reduced by sending voice over IP networks.

Voice over IP VPN is emerging as a viable way to achieve these advantages. The emergence of public and virtual private IP services promises to make it easier for customers, suppliers, and businesses to use data networks to carry voice services. As with any powerful new technology, however, VPNs require skilled management to achieve top performance. The highest network performance becomes imperative when the VPN network must deliver high-quality voice communication. Not all IP networks can meet these quality requirements today. For instance, the public Internet is a transport option for voice communication only when reduced voice performance is acceptable, and global reach has the highest priority. When high voice quality is a requirement, ISPs and Network Service Providers (NSPs) can provide other VPN connections that meet required Service Level Agreements (SLAs).

Managing IP Telephony VPN issues

This section provides information on communications security, firewall technologies, and network management as related to VPN issues.

Communication security

The public nature of the Internet, its reach, and its shared infrastructure provide cost savings when compared to leased lines and private network solutions. However, those factors also contribute to make Internet access a security risk. To reduce these risks, network administrators must use the appropriate security measures.

It is important to note that a managed service can be implemented either as a premises-based solution or a network-based VPN service. A premises-based solution includes customer premises equipment (CPE) that allows end-to-end security and Service Level Agreements (SLAs) that include the local loop. These end-to-end guarantees of quality are key differentiators. A network-based VPN, on the other hand, is provisioned mainly by equipment at the service provider's point-of-presence (PoP), so it does not provide equivalent guarantees over the last mile. For a secure VPN that delivers robust, end-to-end SLAs, an enterprise must demand a premises-based solution that is built on an integrated family of secure VPN platforms.

The "private" in virtual private networking is also a matter of separating and insulating the traffic of each customer so that other parties cannot compromise the confidentiality or the integrity of data. IPSec tunneling and data encryption achieves this insulation by essentially carving private end-to-end pipes or "tunnels" out of the public bandwidth of the Internet, and then encrypting the information within those tunnels to protect against someone else accessing the information. In addition to IPSec, there are two standards for establishing tunnels at Layer 2. These are the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP), neither of which includes the encryption capabilities of IPSec. The value of IPSec beyond these solutions is that IPSec operates at IP Layer 3. It allows for native, end-to-end secure tunneling and, as an IP-layer service, it also promises to be more scalable than the connection-oriented Layer 2 mechanisms.

Also, note that IPSec can be used with either L2TP or PPTP, since IPSec encrypts the payload that contains the L2TP/PPTP data. Indeed, IPSec provides a highly robust architecture for secure wide-area VPN and remote dial-in services. It is fully complementary to any underlying Layer 2 network architecture, and with its addition of security services that can protect the VPN of a company, IPSec marks the clear transition from early tunneling to full-fledged Internet VPN services.

An issue, however, is the fact that different implementations of IPSec confer varying degrees of security services. Products must be compliant with the latest IPSec drafts, must support high-performance encryption, and must scale to VPNs of industrial size.

Finally, a VPN platform should support a robust system for authentication of the identity of end users, based on industry standard approaches and protocols.

Firewall technologies

To reduce security risks, appropriate network access policies should be defined as part of business strategy. Firewalls can be used to enforce such policies. A firewall is a network interconnection element that polices traffic the flows between internal (protected) networks and external (public) networks such as the Internet. Firewalls can also be used to “segment” internal networks.

The application of firewall technologies only represents a portion of an overall security strategy. Firewall solutions do not guarantee 100% security by themselves. These technologies must be complemented with other security measures, such as user authentication and encryption, to achieve a complete solution.

The three technologies that are most commonly used in firewall products are packet filtering, proxy servers, and hybrid. These technologies operate at different levels of detail, and thus they provide varying degrees of network access protection. That means that these technologies are not mutually exclusive. A firewall product may implement several of these technologies simultaneously.

Network management and outsourcing models

While enterprises acknowledge the critical role that the Internet and IP VPNs can play in their strategic eBusiness initiatives, they face a range of choices for implementing their VPNs. The options range from enterprise-based or “do-it-yourself” VPNs that are fully built, owned, and operated by the enterprise, to VPNs that are fully outsourced to a carrier or other partner. In the near term, it is generally believed that enterprise-operated and managed VPN services will hover around a 50/50 split, including hybrid approaches.

Increasingly, enterprises are assessing their VPN implementation options across a spectrum of enterprise-based, carrier-based/outsourced, or hybrid models. Each approach offers a unique business advantage.

- **Enterprise based**. This option operates over a public network facility (most commonly the Internet) using equipment that is owned and operated by the enterprise. Its greatest benefit to the enterprise is the degree of flexibility and control it offers over VPN deployment, administration, and adaptability or change.
- **Fully outsourced**. This managed service could be implemented by a collection of partners, including an ISP and a security integration partner. Its advantages include quick deployment, easy global scalability, and freedom from overhead network management.
- **Shared management**. With this hybrid approach, a partner can take responsibility for major elements of infrastructure deployment and management, but the enterprise retains control over key aspects of policy definition and security management.

Conclusion

Moving to a multipurpose packet-based VPN that transports both voice and data with high quality poses a number of significant management challenges. Managers must determine whether to operate the network using an enterprise-based model, an outsourced or carrier-based model, or a hybrid model. They must settle security issues that involve several layers of the network. And they must ensure that they and their vendors can achieve the required QoS levels across these complex networks. Yet the advantages of converged, multipurpose VPNs remain a strong attraction. The opportunity to eliminate separate, duplicate networks and costly dedicated facilities, avoid costly public network long distance charges, and reduce administrative overhead provides a powerful incentive. Most important, by helping integrate voice and data communication, multimedia messaging, supplier and customer relationship management, corporate data stores, and other technologies and resources, converged networks promise to become a key enabler for eBusiness initiatives.

NAT

IP telephony may not work across Network Address Translation (NAT), because if private IP addresses are exchanged in signaling messages these addresses are not reachable from the public side of the NAT and cannot be used for the media sessions.

The problem is not encountered in all VoIP scenarios. It is avoided for VPN-based remote access, and NATs are usually not needed internally within the enterprise network. VoIP has to traverse NAT, usually at the border between the enterprise and a VoIP trunk to a service provider, as well as in hosted VoIP service.

If the network design includes a firewall within the enterprise network to protect certain servers or some part of the network, so that IP telephony traffic has to traverse the internal firewall, then it is preferable that the firewall not perform a NAT function. IP telephony will then work across the firewall once the appropriate ports are open on the firewall. For more information, see *Avaya IP Telephony Implementation Guide:* iImplementation_Guide

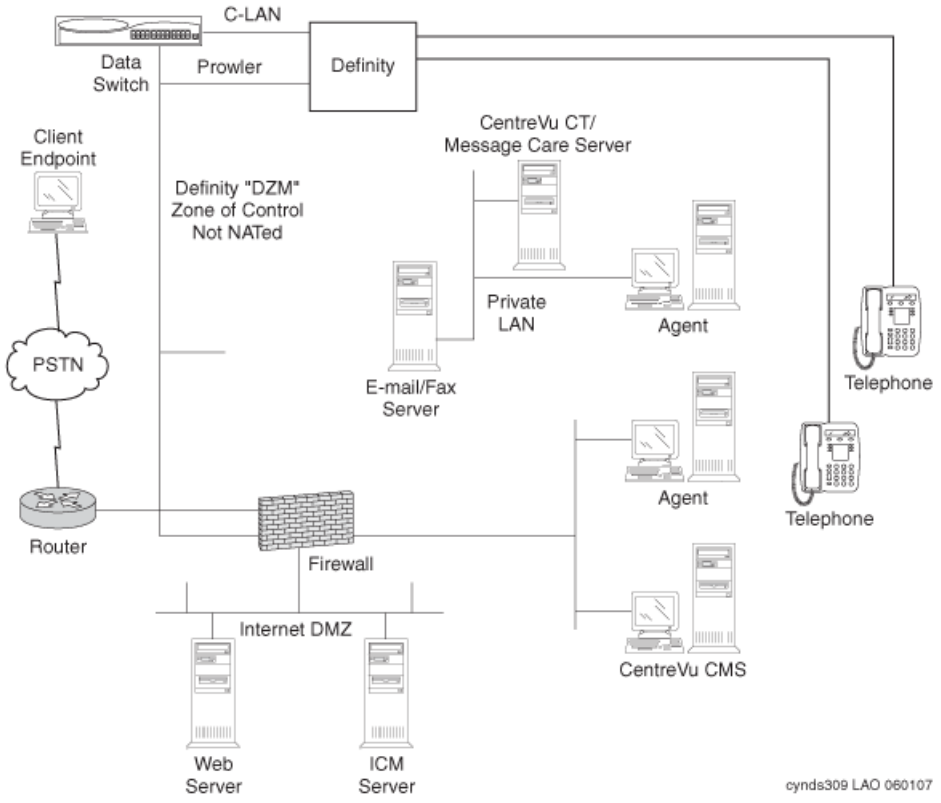
see appendix B for recommendations regarding list of ports).

When connecting the enterprise to an IPT SP through a VoIP trunk — either SIP or H.323 — there will likely be a NAT at the enterprise border. The recommended solution for this scenario is to deploy a Session Border Controller (SBC) near the NAT (for example, in the enterprise DMZ). SBCs from multiple vendors have been tested for interoperability with Avaya's IP Telephony solutions. For a list of Avaya Developer*Connection* members and Avaya compliance-tested solutions, refer to the solutions directory at: www.devconnectprogram.com.

Alternatively, in certain cases an Application Layer Gateway (ALG) can be used. Another alternative is setting up a C-LAN and a Media Processor card in the DMZ, and using Communication Manager as a proxy server between the internal and external networks.

Solutions based on future standards ICE and STUN are expected to be supported in some NAT traversal scenarios where applicable.

Figure 81: IP Telephony without NAT



Converged network design

Converged networks require the application of good management and control practices to support and sustain the deployment of IP telephony. The first step in implementing an IP telephony system is making the commitment to provide a network capable of supporting a real time application such as voice. With many large enterprise networks averaging over 500 hours of downtime per year in 2003 [1], this level of commitment seems to be the exception rather than the rule.

Design and Management

Highly available networks do not just happen. They must be planned and maintained. The probability of success for both of those activities is improved by the application of three fundamental principles -- Simplicity, Manageability and Scalability.

According to an article published in Network World [2] 59% of network downtime was attributable to routing management with approximately 36% of that caused by configuration errors. In another instance a report published by Infonetics Research and reviewed in DMReview [3] attributed the single largest portion (32%) of downtime costs to Application problems with software failure (36%) and human error (22%) precipitating those outages over half of the time. In another article available through Infonetics Research [4] the author cites human error as “the most troubling” cause of outages due to the time and cost of correcting the problems. Older studies [5] attribute as much as 80% of all mission-critical application service downtime to “people or process” failures.

It is clear from the available data that in order to deploy a business-critical IP based service the network upon which it runs must be:

- Easy to configure.
- Easy to monitor and troubleshoot.
- Extensible with minimum reconfiguration. That is, designed with enough resources to grow with the business it supports.

Design for Simplicity

It is self evident that action without understanding is unpredictable. IT staff must interact with the network, so if the system is difficult to understand the probability of error increases. With this thought in mind it is advisable to reduce the number protocols and services on any network segment and reduce the number of decisions the network must make. Simple, documentable, reproducible and verifiable configurations are a must for IP telephony deployment. The IT staff responsible for the network needs to understand how it works, and new staff should be easy to

train. A conscious choice to favor simplicity in design may be the single biggest factor in improving uptime due to its cascading effect on process, documentation and verification.

Design for Manageability

Studies of operator errors have identified several classes of errors typical of network service administrators. Most of these are the result of misconfiguration of new components and unintended actions such as restarts or disabling of hardware while diagnosing problems. Significantly, operators of all experience levels were found to introduce almost all classes of errors with roughly equal frequency.

Research conducted at Rutgers University [6] found that operator action-verification techniques allowed detection and prevention of over half of the errors typically introduced by operators. This data argues strongly for the implementation of reliable change control procedures, and change verification as requisites for highly available networks. To support these activities management tools must be in place to aid in detecting and reporting errors, both for validation of operator actions and diagnosing problems. Network documentation is typically inaccurate and outdated [7] (due in part to lack of change control) so management capabilities to verify configurations are essential.

Design for Scalability

Other researchers have proposed mechanisms for reducing or eliminating the need for operator interaction by automating common tasks. The success of these approaches argues that reducing the scope of changes required to manage and expand network services will pay dividends in network uptime. Excess bandwidth, unused ports and available addresses are required to verify changes and to simplify network expansion. Expansion should begin well before these resources are exhausted.

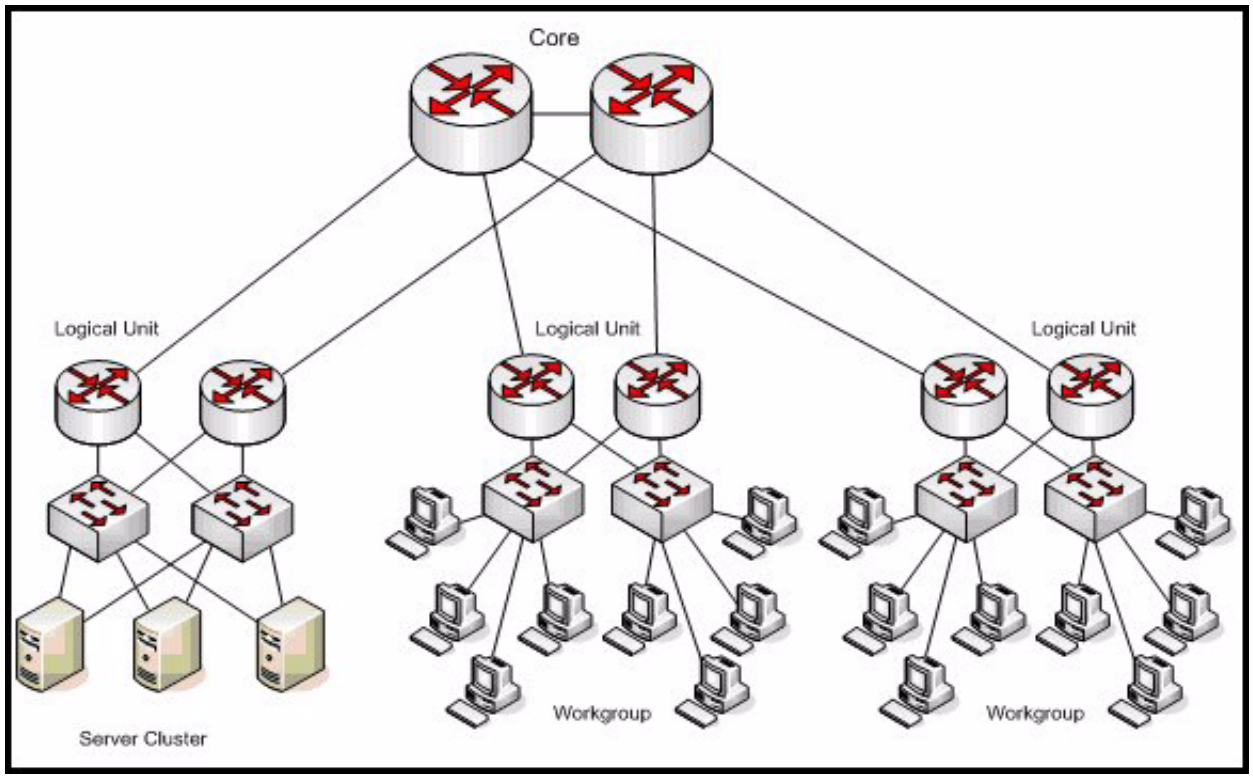
Using designs that limit the impact of changes reduces the potential for errors. For example, if the administrator needs to change both an aggregation switch and a router configuration in order to accommodate new media gateway interfaces, the design has doubled the opportunity for configuration error. If a new subnet needs to be added to Access Control Lists throughout the network core the potential for outage is expanded further still.

The same principles used to reduce software complexity and improve software reliability are applicable to the network complexity problem. Modularity, design reuse, and testability are all attributes of highly reliable networks.

Topologies

The network topology most commonly recommended consists of a redundant core with building blocks of layered routers and switches as shown in the figure below. This is the defacto standard for network design supporting both modularity and reuse.

Figure 82: Typical Network Topology Design

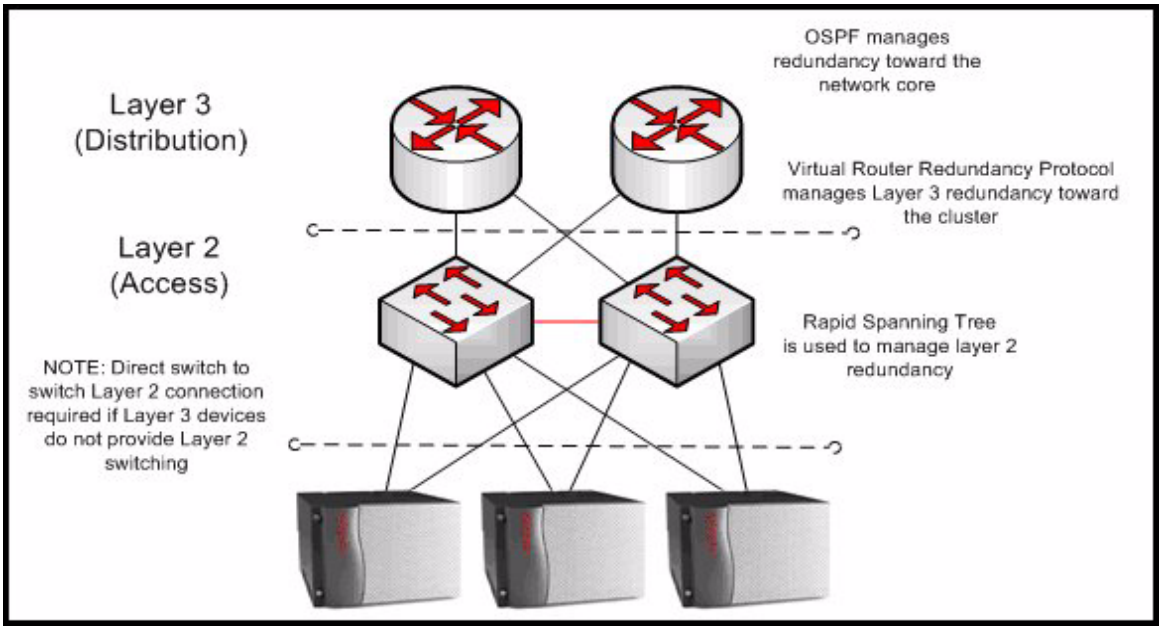


Of course, real networks are far more complex with many more nodes and services. In addition, real deployments typically have legacy constraints, multiple sites, and heterogeneous equipment. It is beyond the scope of this document to detail solutions for the potential configurations of entire networks. To address those issues, Avaya provides a full range of service offers from assessment to outsourced management. Please visit the Avaya web site for further information regarding these services.

Server Cluster

A review of the server cluster configuration as applied to a set of G650 IP-connected port networks will serve to illustrate the principles discussed and validate the modular topology.

Figure 83: Layered Server Cluster Topology



Assume that each G650 is equipped with redundant TN2602AP Media Resource 320 circuit packs optionally configured for load balancing or IP bearer duplication. Each G650 is also assumed to contain duplicated TN2312BP IP Server Interfaces (IPSI). The number of TN799DP Control Lan (C-LAN) socket termination boards would be sized to accommodate the devices in the wider network and the call capacity of the cluster, but for this small configuration assume a C-LAN for each G650. Also assume the Layer 3 devices use hardware switching for Layer 3 forwarding and that they are also capable of Layer 2 switching between ports. It is important to remember that IP Telephony LAN traffic consists primarily of smaller (approximately 218 octet) packets and it is the per packet overhead that impacts software based routing. Consider that telephony traffic is roughly an order of magnitude more packets per unit bandwidth than typical web page transfers.

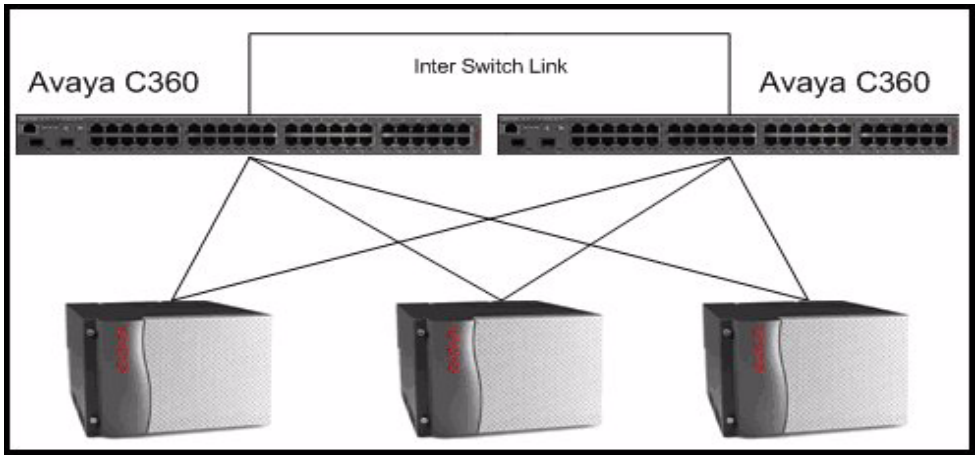
Layers

The obvious question is why there is a separate Layer 2 access level if the devices at the Layer 3 distribution layer are capable of Layer 2 switching? In general, the access layer reduces the complexity of the network block by separating the functions of the devices, and provides scalability when more ports are required as the network grows. To ensure network modularity, the routers serving this cluster should be dedicated to the cluster and sized to the task. Simplification argues for the reduction of subnets and therefore routed interfaces in the cluster since the service is common. If remote IPSIs or multiple server clusters are implemented across the network, using a single subnet within the cluster simplifies the configuration of the entire network. The addition of static subnets in the direction of the cluster [8] increases the

configuration complexity with little benefit in terms of availability unless the subnets terminate on different routers, which in turn implies separate modular clusters. An argument can be made that separate subnets simplify diagnostic activities, but this benefit is achievable with address partitioning within the subnet. Port densities for smaller full featured routers may be inadequate to scale to the connectivity requirements of even this small cluster when the extra ports for management, troubleshooting, and testing are considered.

An alternative design utilizes the smaller high density integrated switching and routing platforms that are becoming popular as routing functions have moved into commodity ASICs. An example using the Avaya C360 stackable switch is shown below.

Figure 84: Integrated high density switch topology

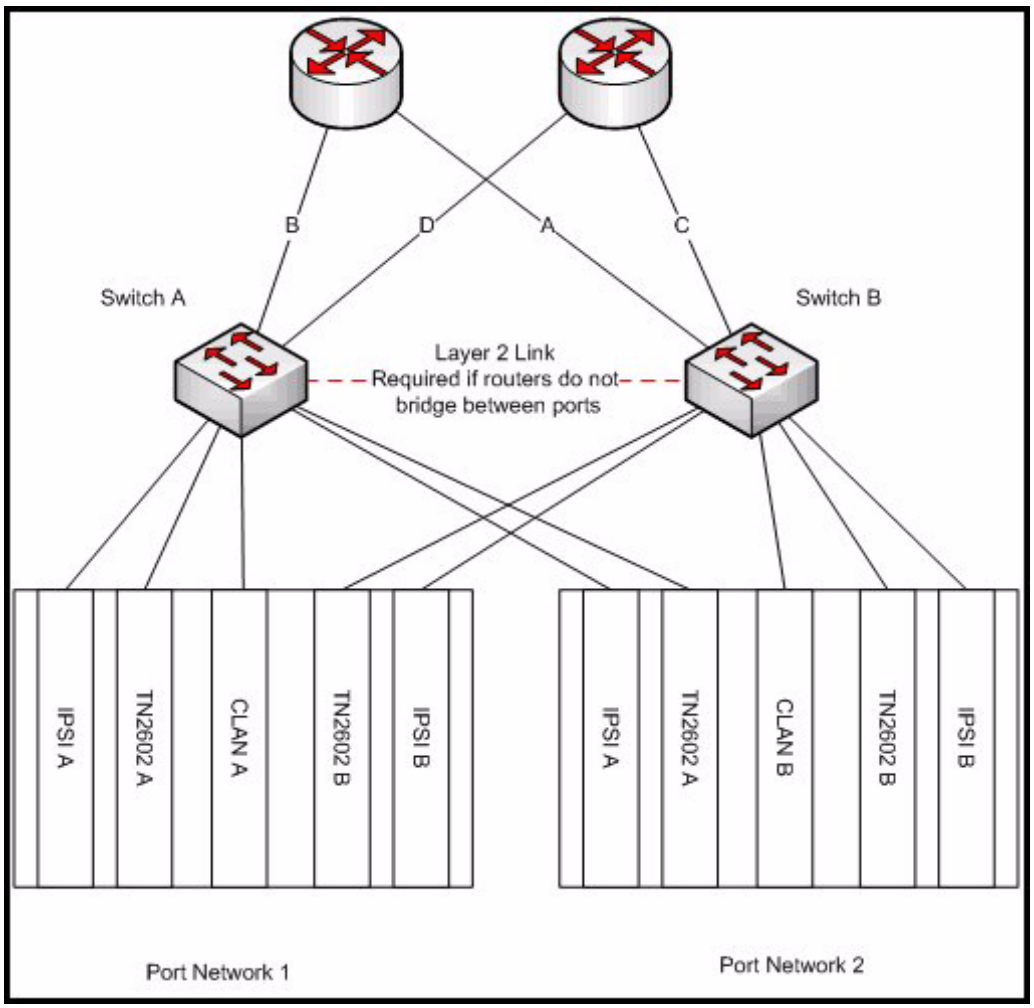


When selecting this type of configuration, bandwidth and inter-switch traffic capacity must be considered. In a load balanced configuration under fault conditions, approximately ½ the call load may travel on the inter-switch link. The inter-switch link must be redundant to prevent a single failure from causing a bifurcated network and, if a Link Aggregation Group (LAG) is used to eliminate potential spanning tree loops, the individual link bandwidth must still be capable of supporting the required traffic.

Redundancy

Hardware redundancy is a proven and well defined tool for increasing the availability of a system. Avaya Critical Availability solutions have traditionally employed this technique to achieve 99.999% availability. One question to consider in the deployment of redundant hardware is symmetric (active-active) or asymmetric (active-standby) configurations. Well known reliability expert Evan Marcus [9] recommends asymmetric configurations for “pure availability.” Avaya’s control network and TDM bearer redundancy solutions follow that model. For IP-PNC designs, bearer duplication supports asymmetric redundancy for bearer flows but symmetric redundancy, or “load balanced” configurations, are the default. Due the inherent complexity of TCP state replication, the C-LAN configurations are always symmetric.

Figure 85: Redundant connections



It is good practice to have the redundant boards of each PN connected to redundant Layer 2 switches as shown to protect each PN from failure of the Layer 2 switch itself. If asymmetric redundancy is configured through IP bearer duplication, it is essential for proper fail over operation that the active and standby TN2602 boards have equivalent Layer 2 connectivity. In the case of IP bearer duplication the secondary TN2602 takes over by assuming both the L2 and L3 address of the connection terminations. This minimizes the disruption due to fail over [10] but requires the network to be configured to accommodate the apparent “move” of an end point from one switch to the other, as it normally would for a spanning tree change.

Layer 2

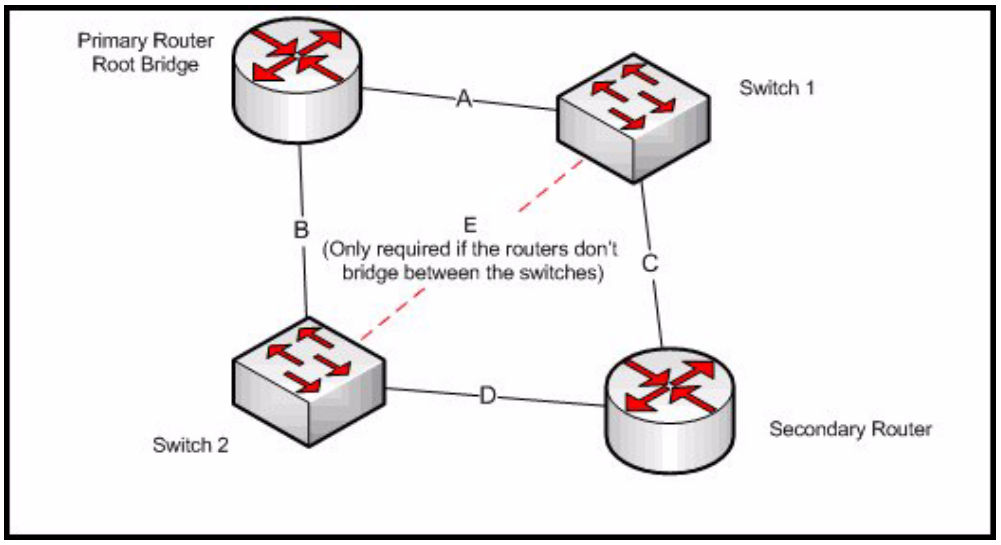
Layer 2 configuration of the switches supporting the cluster should use IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) to prevent loops and for selection between redundant links. Most modern switches implement this protocol. Selecting a device for Layer 2 access that does not support RSTP should be very carefully considered since those devices are likely to be obsolete and lacking in other highly desirable features in areas such as Quality of Service, security, and manageability. RSTP is also preferred over most alternative solutions that are typically not standards based and can cause problems with interoperability, scalability and configuration complexity. Whichever redundancy protocol is selected must be well understood by the IT staff responsible for maintaining the network.

It is good policy to enable RSTP on all ports of the Layer 2 switches, even those ports directly connected to hosts. Remember that misconfiguration and human error are more likely to occur than link failure and the added protection of loop avoidance is worth the minimal overhead. This is an additional argument in favor of RSTP as the redundancy protocol to use since other solutions may not be applicable uniformly to the subnet.

With modular configuration the spanning tree itself is kept simple and deterministic. Consider the sample spanning tree configuration in the figure below. The topology has been redrawn and the host connections have been removed to simplify the explanation. Assume the bridge priorities are assigned such that the VRRP primary router has the highest priority, the secondary router is next, Switch 1 is third, and Switch 2 is last. It is also important that the bandwidth of all links be equivalent and adequate to handle the aggregated traffic.

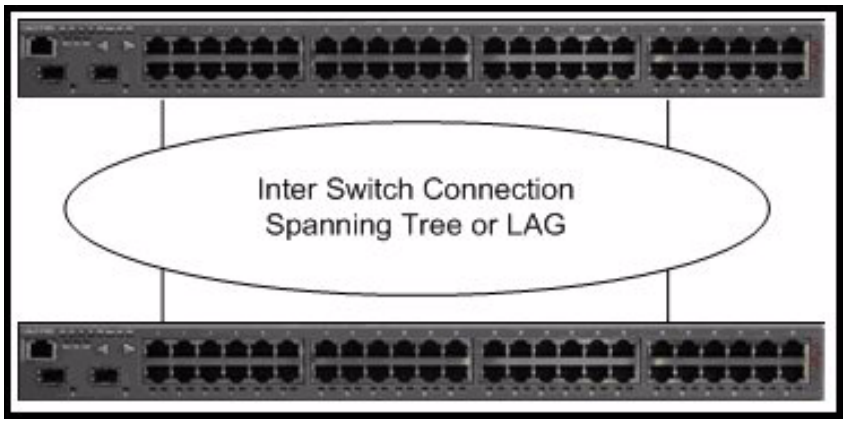
In the example below, links A and B are directly attached to the root bridge so they will be forwarding. Link C connects to a higher priority bridge than link D, so link D will be disabled and Switch 1 will be the designated root for the secondary router. In this configuration, traffic from the attached devices flows directly to the primary router on links A & B.

Figure 86: Sample spanning tree



If the primary router fails, the secondary router becomes both the active router and the root bridge, and traffic from the switches flows on the reconfigured spanning tree along links C & D. If bridge priorities are not managed, traffic from one switch may be directed through the secondary router and the other switch as normal operation.

Figure 87: Alternate configuration - Layer 2



In the alternate integrated device configuration, bridge priority is less significant but other factors may add to complexity. In particular, link sizing becomes an issue if there are not enough Gigabit Ethernet aggregation ports. If a link aggregation group (LAG) is used, flow distributions must be understood to ensure correct behavior.

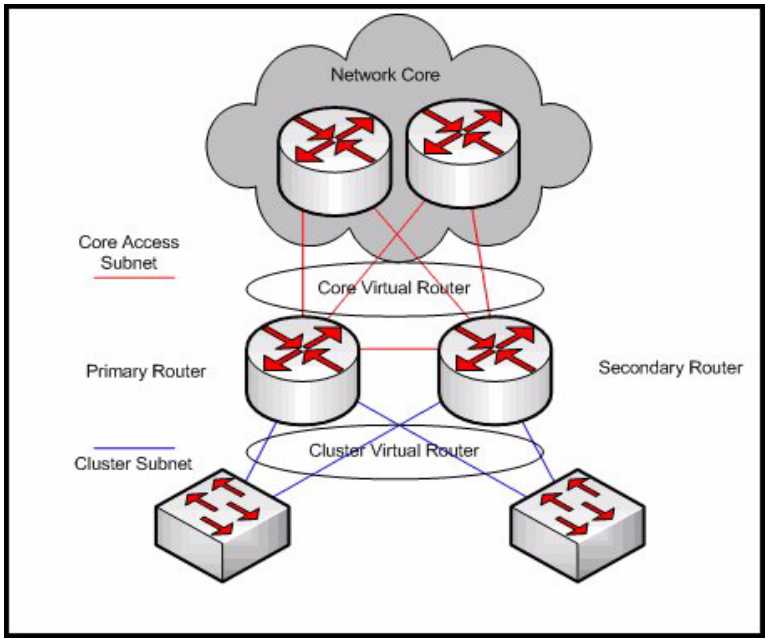
Layer 3

The symmetric or asymmetric question is linked to the configuration of redundancy for the routers serving this cluster. If the single subnet model is used, the router configuration in the direction of the cluster will also follow the asymmetric model. Virtual Router Redundancy (VRRP) [11] will be configured with one router as the primary, and the other router as the secondary. If multiple subnets are configured, it is common practice to make one router the primary for some of the subnets and the other router as the primary for the rest. Note that VRRP should be configured with a failover latency greater than the latency required for the Layer 2 loop avoidance protocol to prevent LAN failures from perturbing the wider network. Typical defaults are between two and three seconds, which should be adequate in a simple well configured spanning tree.

The cluster subnet is exported to OSPF through the interfaces to the core so that the devices are reachable, but OSPF needs to know which router interface to use for the packets directed to the cluster. Proper operation requires that the link to the primary router is also the preferred OSPF path. If the primary router fails in such a way that the link to the core is not brought down, packets will not reach the cluster until the neighbor adjacency times out. Making these timeouts too small makes the protocol overly sensitive, and may still provide inadequate results.

Alternative configurations with static routes and VRRP operating in the direction of the core have also been proposed. The probability of a VRRP interchange that occurs asymmetrically [12] is arguably lower than a router failure that leaves the physical link state unchanged. Combining that observation with the benefit of decoupling route core disruption from local failure are arguments for this configuration.

Figure 88: VRRP configured for Core Access



References for Converged network design on page 304

1. Infonetics 2/11/2004.
2. Network World 10/26/2004.
3. DMreview 2/18/2004.
4. Medium businesses lose $867,000 a year to network downtime 3/09/2006.
5. Gartner Research 7/03/2001.
6. Understanding and Dealing with Operator Mistakes in Internet Services, USNIX 10/04/2004.
7. Enterprise Computing and Networking, Yankee Group 11/2004.
8. A separate management subnet would be expected, but is unrelated to the service address configuration.
9. Marcus, Stern Blueprints for High Availability, Wiley & Sons 2000.
10. Moving the L2 address to the standby device limits the disruption to the address forwarding tables of the L2 switches, which are designed to accommodate rapid connectivity moves. Gratuitous ARP'ing to rebind the L2 address at the termination level requires all connected devices to update their forwarding tables and increases the scope and interdependency of the perturbation.
11. See the discussion of VRRP and equivalent protocols in the section on Layer 3 availability mechanisms.
12. Some implementations address this by allowing the link state of different interfaces to be coupled. These techniques are also applicable to the OSPF solution, but are typically proprietary.

Quality of Service guidelines

This chapter contains guidelines for deploying Quality of Service (QoS) for an IP Telephony network. This chapter begins with an overview of Class of Service (CoS) versus QoS.

Class of Service refers to mechanisms that tags traffic in such a way that the traffic can be differentiated and segregated into various classes. *Quality of Service* refers to what the network does to the tagged traffic to give higher priority to specific classes. If an endpoint tags its traffic with Layer 2 802.1p priority 6 and Layer 3 Differentiated Services Code Point (DSCP) 46, for example, the Ethernet switch must be configured to give priority to value 6, and the router must be configured to give priority to DSCP 46. The fact that certain traffic is tagged with the intent to give it higher priority does not necessarily mean it will receive higher priority. CoS tagging does no good without the supporting QoS mechanisms in the network devices.

Topics covered in this section include:

CoS

IEEE 802.1p/Q at the Ethernet layer (Layer 2) and DSCP at the IP layer (Layer 3) are two standards-based CoS mechanisms that are used by Avaya products. These mechanisms are supported by the IP Telephone, the S8300 Server, and the C-LAN and Media Processor circuit packs. Although TCP/UDP source and destination ports are not CoS mechanisms, they can be used to identify specific traffic, and can be used much like CoS tags. Other non-CoS methods to identify specific traffic are to key in on source and destination IP addresses and specific protocols, such as RTP. The Media Processor circuit pack and IP Telephones use RTP to encapsulate audio.

Note that the 802.1Q tag changes the size and the format of the Ethernet frames. Because of this, many switches must be explicitly configured to accept 802.1Q tagged frames. Otherwise, these switches might reject the tagged frames. The two fields to be concerned with are the Priority and Vlan ID (VID) fields. The Priority field is the “p” in 802.1p/Q, and ranges in value from 0 to 7. (*802.1p/Q* is a common term that is used to indicate that the Priority field in the 802.1Q tag has significance. Prior to real-time applications, 802.1Q was used primarily for VLAN trunking, and the Priority field was not important.) The VID field is used as it always has been, to indicate the VLAN to which the Ethernet frame belongs.

The IP header with its 8-bit Type of Service (ToS) field, which was, and in some cases still is, originally used. This original scheme was not widely used, and the IETF developed a new Layer 3 CoS tagging method for IP called Differentiated Services (DiffServ, RFC 2474/2475). DiffServ uses the first 6 bits of the ToS field, and ranges in value from 0 to 63. Table 52: Comparison of DSCP with original TOS shows the original ToS scheme and DSCP in relation to the 8 bits of the ToS field.

Table 52: Comparison of DSCP with original TOS

8-bit ToS field							
IP precedence bits			**ToS bits**				**0**
0	1	2	3	4	5	6	7
DSCP bits						0	0

Ideally, any DSCP value should map directly to a precedence and traffic parameter combination of the original scheme. This is not always the case, however, and it can cause problems on some older devices.

On any device, new or old, a nonzero value in the ToS field has no effect if the device is not configured to examine the ToS field. Problems arise on some legacy devices when the ToS field is examined, either by default or by enabling QoS. These legacy devices (network and endpoint) might contain code that implemented only the precedence portion of the original ToS scheme, with the remaining bits defaulted to zeros. This means that only DSCP values that are divisible by 8 (XXX000) can map to the original ToS scheme. For example, if an endpoint is tagging with DSCP 40, a legacy network device can be configured to look for precedence 5, because both values show up as 10100000 in the ToS field. However, a DSCP of 46 (101110) cannot be mapped to any precedence value alone. Another problem is if the existing code implemented precedence with only one traffic parameter permitted to be set high. In this case, a DSCP of 46 still does not work, because it requires 2 traffic parameter bits to be set high. When these mismatches occur, the older device mighty reject the DSCP tagged IP packet, or exhibit some other abnormal behavior. Most newer devices support both DSCP and the original ToS scheme.

Layer 2 QoS

On Avaya and Cisco switches, IP Telephony traffic can be assigned to higher priority queues. The number and the sizes of queues and how the queues function are device dependent, and beyond the scope of this document.

However, in general, a fixed number of queues exist, and the queues are usually not configurable. If the queues are configurable, it is typically not recommended. Older or lower end switches commonly have only two queues or none at all. Newer or higher-end switches commonly have four or eight queues, with eight being the maximum because there are only eight Layer 2 priority levels. When configured to do so, the Ethernet switch can identify the high-priority traffic by the 802.1p/Q tag, and assign that traffic to a high-priority queue. On some switches, a specific port can be designated as a high-priority port, which causes all traffic that originates from that port to be assigned to a high-priority queue.

Layer 3 QoS

It is usually more complicated to implement QoS on a router than on an Ethernet switch. Unlike Ethernet switches, routers do not just have a fixed number of queues. Instead, routers have various queuing mechanisms. For example, Cisco routers have standard first-in first-out queuing (FIFO), weighted fair queuing (WFQ), custom queuing (CQ), priority queuing (PQ), and low-latency queuing (LLQ). LLQ is a combination of priority queuing and class-based weighted fair queuing (CBWFQ), and it is Cisco's recommended queuing mechanism for real-time applications such as IP Telephony. Each queuing mechanism behaves differently, is configured differently, and has its own set of queues.

First, the desired traffic must be identified using DSCP, IP address, TCP/UDP port, or protocol. Then the traffic must be assigned to a queue in one of the queuing mechanisms. Then the queuing mechanism must be applied to an interface.

The interface itself might also require additional modifications, independent of the queuing mechanism, to make QoS work properly. For example, Cisco requires traffic shaping on Frame Relay and ATM links to help ensure that voice traffic is allotted the committed or guaranteed bandwidth. Cisco also recommends link fragmentation and interleaving (LFI) on WAN links below 768 kbps, to reduce serialization delay. Serialization delay is the delay that is incurred in encapsulating a packet and transmitting it out the serial interface. It increases with packet size, but decreases with WAN link size. The concern is that large low-priority packets induce additional delay and jitter, even with QoS enabled. This is overcome by fragmenting the large low-priority packets and interleaving them with the small high-priority packets, thus reducing the wait time for the high-priority packets. Table 53: Serialization delay matrix on page 318 lists

serialization delay for a variety of packet sizes and line speeds. The formula for determining serialization delay is:

$$\text{Serialization Delay} = \frac{\text{Packet Size (bits)}}{\text{Line Speed}}$$

Table 53: Serialization delay matrix

WAN line speed	Packet size					
	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes	1500 bytes
56 kbps	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
64 kbps	8 ms	16 ms	32 ms	64 ms	128 ms	187 ms
128 kbps	4 ms	8 ms	16 ms	32 ms	64 ms	93 ms
256 kbps	2 ms	4 ms	8 ms	16 ms	32 ms	46 ms
512 kbps	1 ms	2 ms	4 ms	8 ms	16 ms	23 ms
768 kbps	640 µs	1.28 ms	2.56 ms	5.12 ms	10.24 ms	15 ms

Because of all these configuration variables, properly implementing QoS on a router is no trivial task. However, QoS is needed most on the router because most WAN circuits terminate on routers.

QoS guidelines

There is no all-inclusive rule regarding the implementation of QoS because all networks and their traffic characteristics are unique. It is good practice to baseline the IP Telephony response on a network without QoS, and then apply QoS as necessary. Avaya Network Consulting Services can help with baselining services. Conversely, it is bad practice to enable multiple QoS features simultaneously, not knowing what effects, if any, each feature is introducing.

Generally, for newer network equipment, best practices involve enabling Layer 3 (DiffServ) QoS on WAN links traversed by voice. Tag voice and data with DiffServ Code Point 46 (Expedited Forwarding), and set up a strict priority queue for voice. If voice quality is still not acceptable, or if QoS is desired for contingencies such as unexpected traffic storms, QoS can then be implemented on the LAN segments as necessary.

There is one caution to keep in mind about QoS with regard to the processor load on network devices. Simple routing and switching technologies have been around for many years and have advanced significantly. Packet forwarding at Layer 2 and Layer 3 is commonly done in hardware (Cisco calls this fast switching, with “switching” being used as a generic term here), without heavy processor intervention. When selection criteria such as QoS and other policies are added to the routing and switching process, it inherently requires more processing resources from the network device. Many of the newer devices can handle this additional processing in hardware, and maintain speed without a significant processor burden. However, to implement QoS, some devices must move a hardware process to software (Cisco calls this process "process switching"). Process switching not only reduces the speed of packet forwarding, but it also adds a processor penalty that can be significant. This can result in an overall performance degradation from the network device, and even device failure. Each network device must be examined individually to determine if enabling QoS will reduce its overall effectiveness by moving a hardware function to software, or for any other reason. Since most QoS policies are implemented on WAN links, the following general points for Cisco routers are offered to increase the level of confidence that QoS remains in hardware (consult Cisco to be sure):

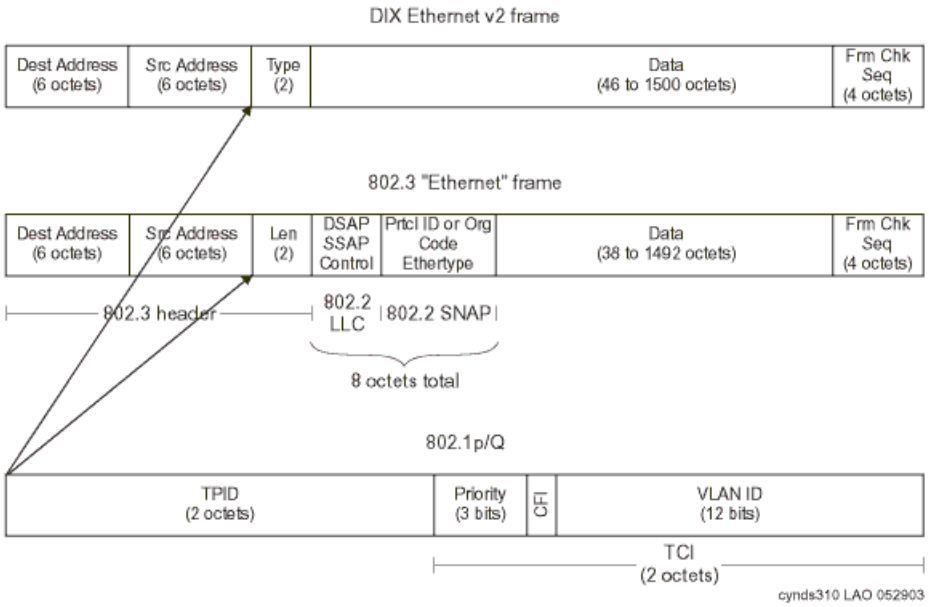
- Newer hardware platforms are required: 2600, 3600, 7200, and 7500
- Newer interface modules (WIC, VIP, and so on) are required. Consult Cisco to determine which hardware revision is required for any given module.
- Sufficient memory is required: device dependent.
- Newer IOS is required: 12.0 or later.

Avaya Layer 3 switches and the X330 WAN module support both 802.1 p/Q and DiffServ QoS.

Several things should be examined whenever QoS is enabled on a network device. First, the network administrator should examine the processor load on the device, and compare it to levels before QoS was enabled. It is likely that the levels will have gone up, but the increase should not be significant. If it is, then it is likely that the QoS process is being done by software. Also, the processor load must remain at a manageable level (50% average, 80% peak). If the processor load is manageable, then the IP Telephony response (for example, voice quality) should be checked to verify that it has improved under stressed conditions (for example, high congestion). If the IP Telephony response has improved, the other applications should be checked to verify that their performances have not degraded to unacceptable levels.

IEEE 802.1 p/Q

Figure 89: 802.1Q tag



The IEEE 802.1Q standard is a Layer 2 tagging method that adds 4 bytes to the Layer 2 Ethernet header. IEEE 802.1Q defines the open standard for VLAN tagging. Two bytes house 12 bits that are used to tag each frame with a VLAN identification number. The IEEE 802.1p standard uses 3 of the remaining bits in the 802.1Q header to assign one of 8 different classes of service. Communication Manager users can add the 802.1Q bytes and set the priority bits as desired. *Avaya suggests that a priority of 6 be used for both voice and signaling*. The Avaya line of data switches can switch frames with or without these VLAN headers, with no configuration time spent. IEEE 802.1p and IEEE 802.1Q are OSI layer 2 solutions, and work on frames.

Because 802.1Q is a Layer 2 (Ethernet) standard, it only applies to the Ethernet header. At every Layer 3 boundary (router hop), the Layer 2 header, including CoS parameters, is stripped and replaced with a new header for the next link. Thus, 802.1Q does not enable end-to-end QoS.

Recommendations for end-to-end QoS

When end-to-end QoS is desired, Avaya recommends using DiffServ, a Layer 3 CoS method. Modern routers can map DiffServ Code Points (DSCP) to 802.1p priority values, so 802.1p tags can be recreated on each Ethernet link. This functionality is supported in Avaya Layer 3 switches, and the X330 WAN module.

IEEE 802.1p states a standard according to which these bits are used for CoS. The precedence is listed in Table 54: IEEE 802.1 precedence and service mapping.

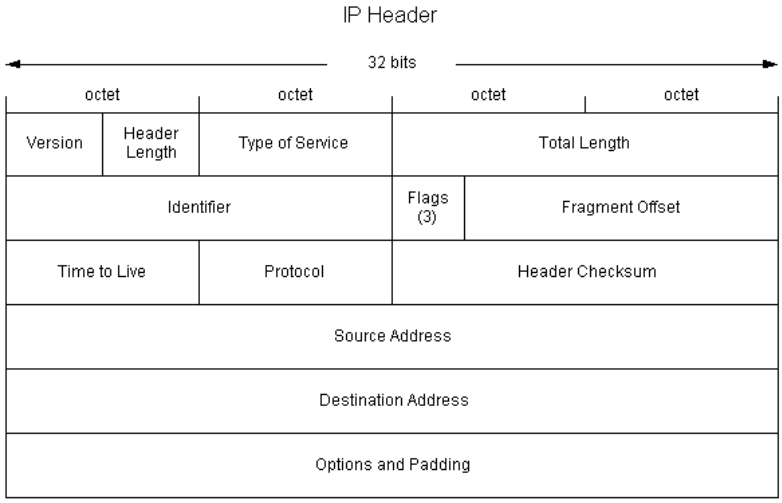
Table 54: IEEE 802.1 precedence and service mapping

User priority	Service mapping
000	Default, assumed to be best effort
001	Reserved, less than best effort
010	Reserved
011	Reserved
100	Delay sensitive, no bound
101	Delay sensitive, 100 ms bound
110	Delay sensitive, 10 ms bound
111	Network control

DiffServ

The Differentiated Services (DiffServ) prioritization scheme redefines the existing TOS byte in the IP header (Figure 90: Differentiated Services (DiffServ) TOS byte on page 322) by combining the first 6 bits into 64 possible combinations. This use of the TOS byte is still evolving, but can be used now by Communication Manager, IP Telephones, and other network elements such as routers and switches in the LAN and WAN.

Figure 90: Differentiated Services (DiffServ) TOS byte



A DiffServ Code Point (DSCP) of 46 (101110), referred to as expedited forwarding (EF), is suggested for the proper treatment of voice packets. Signaling packets can also be marked with DSCP 46 if there is sufficient bandwidth to prevent dropped packets. To assure that voice and signaling packets are not in contention, mark signaling packets with a different DSCP value. With Communication Manager, you can set any DSCP value needed to work with a company's QoS scheme.

Some common DiffServ Code Points are defined in RFCs 2474 and 2475. Although DSCPs are specified in IETF RFCs, the treatment of packets that are tagged with DiffServ depends on implementation.

Note that older routers might require a DSCP setting of 40 (101000), which is backward compatible with the original TOS byte definition of critical. But again, Avaya products and software allows users to set any of the 64 possible DSCP values to work with your voice quality

policy. The TOS byte is an OSI model Layer 3 solution, and works on IP packets on the LAN and possibly the WAN, depending upon the service provider.

Table 55: Original TOS specification

Bit description	Value	Use
Bits 0-2IP precedence	000 001 010 011 100 101 110 111	Routine Priority Immediate Flash Flash Override CRITIC/ECP Internetwork control Network control
Bit 3 delay	0 1	Normal Low
Bit 4 Throughput	0 1	Normal High
Bit 5 reliability	0 1	Normal High
Bit 6 monetary cost	0 1	Normal Low
Bit 7 reserved		Always set to 0

RSVP

Resource Reservation Protocol (RSVP) is a protocol that hosts can use to request specific QoS parameters through the network for a particular application data stream. A host can request guaranteed service through a network. If all routers have RSVP support enabled, and if there exists sufficient unreserved bandwidth, a reservation is established throughout the network. If insufficient bandwidth exists, the reservation fails and notifies the hosts. At that point, hosts can choose to send traffic without a reservation, or drop the connection.

RSVP is supported in Communication Manager beginning with Release 1.3. RSVP can be enabled per network region on the network region form. If RSVP is enabled, endpoints including IP Telephones and media processors attempt to establish a reservation for each call. If the reservation fails, Avaya endpoints still try to place a call, but lower the DiffServ priority of the call

to the better-than-best-effort (BBE) DSCP that is defined on the network region form. By default, this value is 43.

If RSVP is enabled on a network region, it is very important that it also be enabled on associated routers. If not, all RSVP reservations fail, and all voice traffic in that region is marked with the BBE DSCP, which will generally receive degraded service versus the EF (DSCP 46) DiffServ Code Point.

Queuing methods

This section discusses common queuing methods and their appropriateness for voice.

WFQ

Weighted fair queuing (WFQ) is similar to first in, first out (FIFO) queuing, except that it grants a higher weight to small flows, and flows that are marked with higher DiffServ or IP TOS priorities. This queuing strategy does allow smaller (for example, telnet) and higher-priority (for example, IP Telephony) protocols to squeeze in before high-flow (for example, ftp) packets, but does not starve off any traffic. By itself, it is not appropriate for IP Telephony traffic because high-flow traffic can still delay IP Telephony traffic, and cause unacceptable latency and jitter.

PQ

Strict priority queuing (PQ) divides traffic into different queues. These queues are usually high, medium, normal, and low, based on traffic type. This form of queuing services the queues in order of priority, from high to low. If there is a packet in the high-priority queue, it will always be serviced before the queue manager services the lower-priority queues. With priority queuing, however, it is possible to starve out lower-priority flows if sufficient traffic enters the high-priority queue. This mechanism works very well for IP Telephony traffic (where IP Telephony bearer and signaling are inserted in the high-priority queue), but might work less well for routine data traffic that is starved out if sufficient high-priority traffic arrives.

Round-robin

Round-robin (sometimes called *custom*) queuing sorts data into queues, and services each queue in order. An administrator manually configures which type of traffic enters each queue, the queue depth, and the amount of bandwidth to allocate to each queue.

Round-robin queuing is not particularly suited to IP Telephony. It does not ensure strict enough priority to voice packets, so they may still wait behind other traffic flows in other queues. Latency and jitter can be at unacceptable levels.

CB-WFQ / LLQ / CBQ

Class-Based Weighted Fair Queuing (CB-WFQ) with Low-Latency Queuing (LLQ), which is sometimes called Class-Based Queuing (CBQ), combines the above-mentioned queuing mechanisms. Generally, there is one strict-priority queue, several round-robin queues, and weighted fair queuing for the remainder. This queuing mechanism works very well for converged networks. IP Telephony bearer and signaling packets receive the priority they need, while there remains an equitable mechanism for distributing remaining bandwidth. In addition, limits can be set on the high-priority queue to prevent it from using more than a specified amount of bandwidth. Bandwidth that is reserved for the high-priority queue will be given to other queues if insufficient traffic enters the high-priority queue.

RED / WRED

Although they are not queuing methods *per se*, Random Early Detection (RED) and Weighted Random Early Detection (WRED) are important queue management techniques. RED and WRED work by randomly discarding packets from a queue. RED takes advantage of the congestion control mechanism of TCP. By randomly dropping packets prior to periods of high congestion, RED causes the packet source to decrease its transmission rate. Assuming that the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, which indicates that the congestion is cleared. Some implementations of RED, called Weighted Random Early Detection (WRED), combines the capabilities of the RED algorithm with IP Precedence. This combination provides for preferential traffic handling for higher-priority packets. It can selectively discard lower-priority traffic when the interface begins to get congested, and provide differentiated performance characteristics for different classes of service.

RED and WRED are useful tools for managing “data” traffic, but should not be used for “voice.” Because IP Telephony traffic runs over UDP, because IP Telephony protocols do not retransmit lost packets, and because IP Telephony transmits at a constant rate, the IP Telephony queue should never be configured for WRED. WRED only adds unnecessary packet loss, and consequently reduces voice quality.

Traffic shaping and policing

Traffic shaping is a mechanism to reduce the rate at which data is transmitted over an interface. When people discuss traffic shaping, they are usually referring to the related technology of traffic policing. Policing works by either adjusting the priority of excess traffic to a lower queue, or discarding it. As with RED, discarding TCP traffic has the effect of throttling the stream by forcing window size to shrink, and decreasing its transmission rate. Because RTP is a fixed-bandwidth application, discarding RTP packets reduces voice quality without altering the transmission rate. Adjusting the priority of voice traffic removes the strict priority protection that reduces latency and jitter, and offers the highest voice quality. Thus, in most cases, it is beneficial to use the QoS mechanisms listed above, rather than traffic shaping and policing, to offer the highest quality for voice.

Frame Relay traffic shaping

Traffic shaping is important in technologies that implement virtual circuits (VCs), such as Frame Relay or ATM, where the Committed Information Rate (CIR) might be less than the physical speed of the interface, the port speed. In such scenarios, it is possible for traffic to burst above the CIR. Depending on the Service Level Agreement (SLA), a carrier might mark excess traffic as Discard Eligible (DE), and either delay or discard it if congestion is detected within the network of the carrier. This behavior is unacceptable for voice traffic, which must minimize delay and jitter to achieve optimal voice quality. To solve this issue, Frame Relay traffic shaping gives an administrator tools to limit the transmission rate on a Frame Relay virtual circuit to the CIR.

A popular misconception is that voice traffic can be confined to the CIR, while data traffic can be allowed to burst. Unfortunately, that is not how Frame Relay works. There is not a QoS mechanism for Frame Relay that is negotiated between service providers and customers. Service providers view all traffic equally, and mark any packet that exceeds the CIR as DE, even if the packet is high-priority voice. Thus, the only way to guarantee optimal performance for voice traffic is to restrict the traffic rate to the CIR.

On a Cisco router, do the following to ensure proper handling for voice:

1. Disable Frame Relay adaptive shaping. This technique reduces the CIR in response to backwards explicit congestion notification (BECN) messages from the service provider. Because traffic is being transmitted at the CIR in the first place, it does not need to be throttled.
2. Set cir and mincir to the negotiated CIR. If FRF.12 fragmentation is implemented, reduce the cir and mincir values slightly to account for the fragment headers.
3. Set be, the excess burst rate, to 0
4. Set bc, the committed burst rate, to cir/100. This accounts for at most a 10-ms serialization delay.
5. Apply this map class to an interface, subinterface, or VC.

Thus, the complete configuration for Frame Relay traffic shaping looks like:

```
map-class frame-relay NoBurst
     no frame-relay adaptive shaping
     frame-relay cir 384000! (for a 384K CIR)
     frame-relay mincir 384000
     frame-relay be 0
     frame-relay bc 3840

interface serial 0
     frame-relay class NoBurst
```

Fragmentation

One large cause of delay and jitter across WAN links is serialization delay, or the time that it takes to put a packet on a wire. For example, a 1500-byte FTP packet takes approximately 214 ms to be fed onto a 56-Kbps circuit. For optimal voice performance, the maximum serialization delay should be close to 10 ms. Thus, it can be problematic for a voice packet to wait for a large data packet over a slow circuit. The solution to this problem is to fragment the large data packet into smaller pieces for propagation. If a smaller voice packet comes in, it can be squeezed between the data packet fragments and be transmitted within a short period of time.

The sections that follow discuss some of the more common fragmentation techniques.

MTU

The maximum transmission unit (MTU) is the longest packet (in bytes) that can be transmitted by an interface without fragmentation. Reducing the MTU on an interface forces a router to fragment the large packet at the IP level. This allows smaller voice packets to squeeze through in a timelier manner.

The drawback to this method is that it increases overhead and processor occupancy. For every fragment, a new IP header must be generated, which adds 20 bytes of data. If the MTU is 1,500 bytes, the overhead is approximately 1.3%. If the MTU is shortened to 200 bytes, however, the overhead increases to 10%. In addition, shortening the MTU to force fragmentation increases processor utilization on both the router and the end host that needs to reassemble the packet.

For these reasons, shortening the MTU is only recommended as a last resort. The techniques described later in this section are more efficient, and should be used before changing the values of the MTU. When changing the MTU, size it such that the serialization delay is less than or equal to 10 ms. Thus, for a 384-kbps circuit, the MTU should be sized as follows: 384000 bps

*0.01 second (10 ms)/8 bits/byte = 480 bytes. As the circuit size diminishes, however, care should be taken to never reduce the MTU below 200 bytes. Below that size, telephony signaling and bearer (voice) packets can also be fragmented, which reduces the link efficiency and degrades voice performance.

LFI

Link Fragmentation and Interleaving (LFI) is an enhancement to Multilink PPP (MLP) that fragments packets at the Layer 2 (PPP) level. Fragmenting at the IP layer, as with MTU reduction, forces the addition of a new 20-byte IP header and an 8-byte PPP header. However, fragmenting at the data link (PPP) layer only forces generation of an 8-byte PPP header, which greatly increases the efficiency of the link.

Avaya recommends use of LFI functionality instead of MTU manipulation when transmitting IP Telephony packets over PPP links. As with MTU, Avaya recommends sizing packets so that the serialization delay is approximately 10 ms or less.

FRF.12

FRF.12 is a Frame Relay standard for fragmentation. It works for Frame Relay in the same way that LFI works for PPP, with similar increases in efficiency over MTU manipulation. When implementing a Frame Relay network, Avaya recommends using FRF.12 for fragmentation, and sizing the fragments so the serialization delay is no more than 10 ms.

RTP

RTP header compression is a mechanism that reduces the protocol overhead that is associated with IP Telephony audio packets. It is a function of the network, and not a function of the IP Telephony application. Along with the benefits of using RTP header compression, there are also cautions.

Application perspective

Table 56: Anatomy of 20-ms G.729 audio packet on page 329 shows the anatomy of a 20-ms G.729 audio packet, which is recommended for use across limited bandwidth WAN links. Notice that two-thirds of the packet is consumed by overhead (IP, UDP, and RTP), and only one-third is used by the actual audio.

Table 56: Anatomy of 20-ms G.729 audio packet

IP header	UDP header	RTP header	20 ms of G.729 audio
20 B	8 B	12 B	20 B

It is important to understand that all 20-ms G.729 audio packets, regardless of the vendor, are constructed like this. Not only is the structure of the packet the same, but the method of encoding and decoding the audio itself is also the same. This sameness is what allows an Avaya IP Telephone to communicate directly with a Cisco IP Telephone, or any other IP Telephone, when using matching codecs. The packets from the application perspective are identical.

Network perspective

RTP header compression is a mechanism that routers use to reduce the 40 bytes of protocol overhead to approximately 2 to 4 bytes. Cisco routers use this mechanism, as does the Avaya X330WAN router, which is a module for the P330 chassis. RTP header compression can drastically reduce the IP Telephony bandwidth consumption on a WAN link when using 20-ms G.729 audio. When the combined 40-byte header is reduced to 4 bytes, the total IP packet size is reduced by 60% (from 60 bytes to 24 bytes). This equates to reducing the total IP Telephony WAN bandwidth consumption by roughly half, and it applies to all 20-ms G.729 audio packets, regardless of the vendor.

Recommendations for RTP header compression

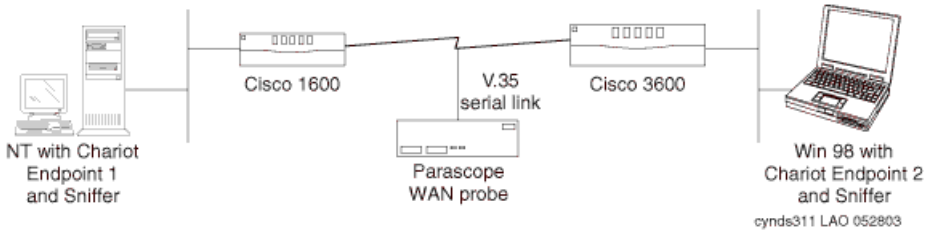
Enterprises that deploy routers that are capable of this feature might be able to benefit from it. However, Cisco recommends caution in using RTP header compression on its routers because it can significantly tax the processor if the compression is done in software. Depending on the processor load before compression, enabling RTP header compression can significantly slow down the router, or cause the router to stop completely. For best results, use a hardware/IOS/ interface module combination that permits the compression to be done in hardware.

RTP header compression has to function with exactness or it will disrupt audio. If for any reason the compression at one end of the WAN link and decompression at the other end do not function properly, the result can be intermittent loss of audio or one-way audio. This has been very difficult to quantify, but there is some anecdotal evidence that cRTP sometimes leads to voice-quality issues. One production site in particular experienced intermittent one-way audio, the cause of which was garbled RTP audio samples inserted by the cRTP device. When, for experimentation purposes, RTP header compression was disabled, the audio problems went away.

RTP header compression test

This section details the results of a simple RTP header compression test that was conducted in a laboratory environment. Although this test was conducted using Cisco routers, the expected behavior is the same for any router that performs this function as specified in RFC 2508. This test was performed in the laboratory configuration that is shown in Figure 91.

Figure 91: Equipment configuration for RTP header compression test



In Figure 91:

- NetIQ Chariot v4.0 was used to simulate IP Telephony calls between the two endpoints. Chariot v4.0 accurately simulates the characteristics of various codecs, and uses a 40-byte IP/UDP/RTP header.
- Sniffer Pro v3.50.02 was used to capture the sent and received packets.
- The Cisco 3600 had IOS v12.1(2)T, and the Cisco 1600 had IOS v12.0(12).
- The Frederick Engineering Parascope WAN probe was tapped into the V.35 serial link to take bandwidth measurements.
- This test was performed using PPP encapsulation on the WAN link.

A single call was placed between the Chariot endpoints using various codecs, all sending 20-ms voice packets.

Table 57 shows the results with and without RTP header compression. *Note that these are rough measurements*.

Table 57: Test call (20ms-packets) results

Codec	Payload bytes per packet	Packets per second	Avg WAN BW consumption (kbps)		% reduction
			without compression	with compression	
G.711 (64 kbps)	160	50	84	68.5	~18%
G.729A (8 kbps)	20	50	27.5	13	~53%
G.723.1 (5.3 kbps)	20	33	18	9	~50%
G.723.1 (6.3 kbps)	24	33	19	10	~47%

For each codec, there was an attempt to verify that the audio packets were received intact. This was done by spot checking the audio packets before and after compression, using two Sniffer protocol analyzers. For every codec except G.711, the RTP header and payload were identical before and after compression. With G.711, however, the received packets had the PADDING flag set in the RTP header, although the flag was not set when the packets were transmitted. The PADDING flag indicates the presence of padding octets at the end of the RTP payload, which cannot be true for G.711.

Configuration

To configure RTP header compression on a Cisco router:

1. Specify the number of RTP connections that can be compressed (cache allocation). In interface configuration mode, the command is **`ip rtp compression-connections`** ***`<number>`***, where
   - The default for ***`<number>`*** is 32, and each call requires two connections.
   - The configurable range is 3 to 256 for PPP and HDLC using IOS v11.3 and later.
   - The configurable range is 3 to 1000 for PPP and HDLC using IOS v12.0(7)T and later.
   - For Frame Relay, the value is fixed at 256.
2. The command to turn on compression is **`ip rtp header-compression`** in interface configuration mode. It must be implemented at both ends of the WAN link. When the command was entered into the router, ip tcp header-compression was also installed automatically. When either command was removed, the other was automatically removed.

See the Cisco documentation for more specific configurations on other types of WAN links (that is, Frame Relay and ATM). Configuration for the X330WAN router is very similar to Cisco, and is well documented in the X330WAN User Guides. For this documentation, see the P330 section at:

http://www.avaya.com/support

Examples of QoS implementation

This section contains sample commands for QoS implementation on Avaya products and Cisco products.

Examples given include:

- Example 1: Cisco router configuration for point-to-point WAN links
- Example 2: C-LANS cannot tag their traffic
- Example 3: More restrictions on the traffic
- Converged infrastructure LAN switches

Example 1: Cisco router configuration for point-to-point WAN links

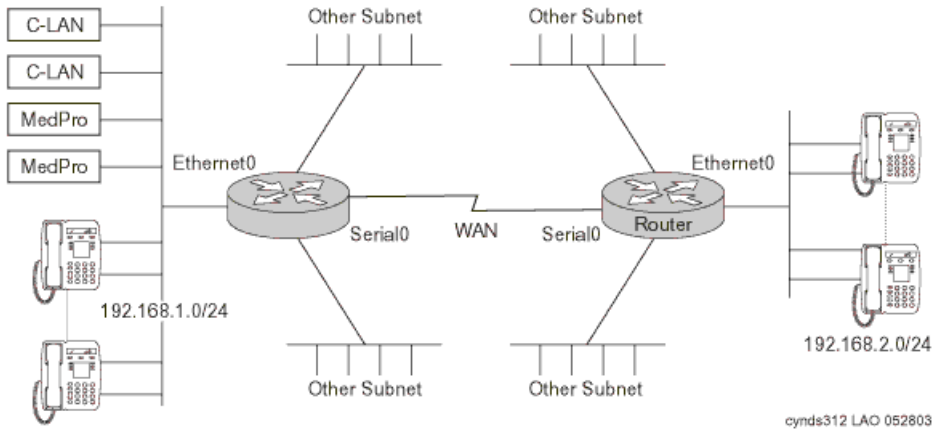
There is a three-step process to turn on QoS on a Cisco router:

1. Set up a class map that defines “interesting traffic” to be prioritized.
2. Select a queuing strategy. In this case, use a policy map to set priority. Set up a route map that sets the priority level (critical).
3. Apply the policy map to an interface.

In Figure 92: High-quality service across a congested WAN link on page 333, set priority-aware Class-Based Weighted Fair Queuing (CB-WFQ) with Low Latency Queuing (LLQ). Although there are more aggressive QoS strategies, they can have a severe impact on data performance. Those other strategies, including Priority Queuing, Custom Queuing, and RSVP, can be implemented at a later date, if conditions warrant. This is a good starting point.

Figure 92: High-quality service across a congested WAN link on page 333 is used as a reference point. The objective is to assure high quality of service to IP Telephony applications across the congested WAN link.

Figure 92: High-quality service across a congested WAN link



CB-WFQ/LLQ is a priority-aware queuing strategy that has a strict priority queue for voice packets, and does round-robin queuing for other types of traffic. Non-prioritized traffic is still forwarded, however, so this should not interfere with a customer's data network. Use weighted random early detect to manage the fair queue.

The actual router configuration used for this testing follows. First, set the endpoints to tag interesting traffic as DSCP 46. Cisco routers support DiffServ in IOS 12.0 and later. Next, set up a class map to match traffic that is marked with DSCP 46. Once traffic is defined by the class map, set policies for it using a policy map. For the policy map to take effect, it has to be applied to an interface. Queue packets on the outgoing interface. In the sample configuration, 768 K of bandwidth is reserved for RTP. This value should be set at or above the maximum bandwidth to be used for IP Telephony. In our case, 768 K supports 9 calls using G.711, or 31 calls using G.729. This example should work well in most cases using Cisco routers with point-to-point WAN links. Networks that use Frame Relay might need additional steps.

Assumptions for Example 1

Suppose all endpoints are capable of tagging with DSCP 46, which is the default for audio. This would be true in a Communication Manager system with *TN799DP C-LAN circuit packs running firmware v5 or later*. Previous firmware versions and the TN799C circuit pack cannot tag at Layer 2 or Layer 3. A matching set of configurations is applied to both routers.

Administration commands for Example 1

Table 58: Administration commands for Example 1

Command	Meaning
`1.class-map match-any VoIP`	Create a class map called “VoIP.”
`2.match ip dscp 46`	Any packet with DSCP 46 is in the class “VoIP.”
`3.policy-map voipQoS`	Create a policy map called “voipQoS.”
`4.class VoIP priority 768`	Give strict priority to packets in the class “VoIP” on up to 768 k of this WAN link.
`5.class class-default fair-queue`	Put everything else in the default class, and transmit it out the default queue in a fair queue fashion.
`6.random-detect dscp-based`	If the default queue starts to get full, randomly discard packets in this queue based on DSCP. The lower values are discarded first.
`7.interface Serial0 description T1 ip address 172.16.0.1 service-policy output voipQoS`	Apply the “voipQoS policy” outbound on this interface.

Example 2: C-LANS cannot tag their traffic

Assumptions for Example 2

- The C-LANs 192.168.1.10 and.11 cannot tag their traffic (TN-799C or earlier).
- The configuration commands in Table 59 are applied only to the left router.

Administration commands for Example 2

Table 59: Administration commands for Example 2

Command	Meaning
`1.access-list 101 permit ip host 192.168.1.10 192.168.2.0 0.0.0.255`	The command “access-list 101...” permits any IP traffic from the 2 C-LANs to the 192.168.2.0/24 network. There is an implicit “deny any” at the end of this access list.
`2.access-list 101 permit ip host 192.168.1.11 192.168.2.0 0.0.0.255`	
`3.class-map match-any untaggedVoIP`	Create a class map called “untaggedVoIP.”
`4.match access-group 101`	Packets that match access list 101 are in the class that is “untaggedVoIP.”
`5.policy-map setDSCP`	Create a policy map called “setDSCP.”
`6.class untaggedVoIP set ip dscp 46`	For all packets in the class “untaggedVoIP,” set the DSCP to 46.
`7.interface Ethernet 0/0 service-policy input setDSCP`	Apply the “setDSCP” policy inbound on this interface.

Example 3: More restrictions on the traffic

Assumptions for Example 3

- DSCP 46 is used throughout to simplify the access list.
- A somewhat matching set of configurations is applied to both routers.

Administration commands for Example 3

Table 60: Administration commands for Example 3

Command	Meaning
`1.access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 dscp 46`	Left router
`2.access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 dscp 46`	Right router The “access list 101...” permits any IP traffic that is tagged with DSCP 46 between the two VoIP subnets. There is an implicit deny any at the end of this access list
`3.class-map match-any VoIP`	Create a class map called “VoIP.”
`4.match access-group 101`	Only packets matching access list 101 are in the class VoIP; this is more restrictive than matching any packet with DSCP 46 or 34.
`5.policy-map voipQoS`	Create a class map called “VoIP.”
`6.class VoIP priority 768`	Give strict priority to packets in the class “VoIP” on up to 768k of this WAN link.
`7.class class-default fair-queue`	Put everything else in the default class and transmit it out the default queue in a fair queue fashion.

Table 60: Administration commands for Example 3

Command	Meaning
`8.random-detect dscp-based`	If the default queue starts to get full, randomly discard packets in this queue based on DSCP (lower values get discarded first).
`9.interface Serial0 description T1 ip address 172.16.0.1 service-policy output voipQoS`	Apply the “voipQoS” policy outbound on this interface.

If any of the endpoints are incapable of tagging, the “dscp 46” can be removed from access list 101. Then any traffic between the two IP Telephony subnetworks, regardless of the tag, is in the class “VoIP.”

Converged infrastructure LAN switches

X330 WAN Module

The new X330WAN versions contain a predefined queue management strategy for IP Telephony that is called CBQ. Use the following procedure to activate CBQ:

Table 61: X330 WAN Module administration commands

Command	Meaning
`1.set qos policy-source local`	Define DSCP-CoS mapping.
! no external policy source	
`2.ip access-list-name 100 voice`	set up access-list 100 with name “voice”.
`3.ip access-list-dscp operation 100 34 fw7`	The X330 WAN has four queues with eight behaviors. fw6 and fw7 are different behaviors within the top strict priority queue.
`4.ip access-list-dscp operation 100 46 fw6`	In access-list 100, map DSCP 46 to the fw6 queue.

1 of 2

Table 61: X330 WAN Module administration commands (continued)

Command	Meaning
5.ip access-list-dscp trust 100 trust-cos-dscp	Trust packet tagging.
6.interface FabricFastEthernet 1	Activate the above mapping on ingress traffic to the Fabric Fast Ethernet interface
7.ip access-group 100 in	Apply the ACL to traffic that is arriving on the FabricFastEthernet port.
8.exit	
9.interface Serial 1	Apply the following commands to Interface Serial 1.
10.voip-queue	Activate “VoIP queue management mode” on the serial interface.
11.exit	
12.interface Serial 1	Apply the following commands to Interface Serial 1.
13.ip rtp header-compression	Enable cRTP (optional).
	2 of 2

Network recovery

Conventional wisdom holds that network reliability is typically 3-9s (99.9%) on a LAN, and 2-9s (99%) on a WAN. The leading causes of network failure are a WAN link failure, administrator error, cable failure, issues that involve connecting new devices or services, and malicious activity, including DoS attacks, worms, and viruses. Somewhere lower down on the list are equipment failures. To achieve the highest levels of availability, it is important that a strong change control policy and network management strategy be implemented.

There are numerous techniques for improving the reliability of data networks, including spanning tree, self-healing routing protocols, network management, and change control. This section discusses the following techniques:

- Change control
- Layer 2 mechanisms to increase reliability
- Layer 3 availability mechanisms
- Dial backup
- Convergence times
- The Converged Network Analyzer

Change control

Change control describes a process by which an organization can control non-emergency network changes, and reduce the likelihood of administrator errors that cause network disruption. It involves carefully planning for network changes (including back-out plans), reviewing proposed changes, assessing risk, scheduling changes, notifying affected user communities, and performing changes when they will be least disruptive. By implementing a strict change control process, organizations can reduce the likelihood of administrator errors, which are a major cause of network disruption, and increase the reliability of their networks.

Layer 2 mechanisms to increase reliability

Spanning tree

IEEE 802.1D spanning tree is an Ethernet loop avoidance protocol. It allows network managers to connect redundant network links within their networks. Prior to the advent of spanning tree, loops within a switched Ethernet network would forward traffic around the loop forever, which saturated the network and prevented new traffic from getting through. Spanning tree selects one switch as a root and creates a loop-free topology connecting to the root. If loops are discovered, one switch blocks that port until its alternate path to the root is disrupted. Then the blocked port is brought back into service. There are several drawbacks to spanning tree:

- By default, all switches have the same priority, which means that root bridge selection can be suboptimal in a network.
- Spanning tree is slow to converge. It typically takes at least 50 seconds from link failure for a backup link to become active. As Layer 2 complexity increases, so does convergence time.
- Although there are mechanisms for speeding up spanning tree, most are proprietary.
- Traditional spanning tree is not VLAN aware. Thus, it will block links even if VLAN provisioning would have prevented a loop.

To solve these issues, the IEEE has recently introduced 802.1s and 802.1w enhancements. 802.1w introduces rapid spanning tree protocol (RSTP). RSTP uses active handshaking to speed up convergence times. 802.1s introduces multiple spanning trees (MST), which is a way of grouping different VLANs into different spanning tree instances. These features might not be present in data network switches yet, but look for them soon.

Link Aggregation Groups

Link Aggregation Groups (LAGs) are a mechanism for combining multiple real inter-switch links (typically four, Avaya products are configurable from two to eight) into one point-to-point virtual interswitch link. The advantage of this mechanism over spanning tree is that an organization can have the redundant links in if a failure occurs in one of the LAG links, the two switches will quickly discover it, and remove the failed link from the LAG., which reduces the convergence time to nearly instantaneous. Not all implementations interoperate, so care must be taken when the LAG connects switches from multiple vendors. Also, LAG links are a point-to-point technology. They cannot be used to connect a backup switch in case the primary fails. When available, this is a very good mechanism for improving the resiliency of LANs.

Layer 3 availability mechanisms

Routing protocols

Routing protocols allow routers to dynamically learn the topology of the network. Should the topology of the network change, routing protocols update their internal topology table, which allows them to route around failure.

There are two types of routing protocol, distance vector and link state. Distance vector protocols, including RIP and IGRP, exchange their entire routing table periodically. To each route, they add their metric (for RIP, this is “hop count”) and insert it in the routing table. If updates fail to arrive before the router’s timer expires, it purges the route and looks for another path. These protocols are usually slow to converge. See Table 62: Sample convergence times (single link failure) on page 343.

Link-state protocols, such as OSPF, take a more holistic view of the network. They compute the entire topology of the network and insert the best path to a destination in the routing table. Link state protocols exchange their routing tables only once, when routers first establish a relationship. After that, they only send updates. They also send hello messages periodically to ensure that the other routers are still present. Link state protocols converge much more quickly than distance vector protocols, and thus are generally better suited to networks that require high availability.

VRRP and HSRP

Virtual Router Redundancy Protocol (VRRP) and the related Cisco proprietary Hot Standby Router Protocol (HSRP) provide a mechanism to deal with router failure without disrupting endpoints on the network. In essence, these protocols work by assigning a virtual IP address and MAC address for the routers. This address is given to endpoints as their default gateway. The two routers send periodic hello messages marked with a priority value between each other. The high-priority router assumes the virtual address, and traffic flows through it. If the primary router fails or its capabilities become degraded (such as if a WAN link fails), the secondary router takes over. This is a useful mechanism to protect endpoints from router failures, and works with IP Telephony endpoints.

Multipath routing

Modern routers and Layer 3 switches allow multiple routes for a particular destination to be installed in the routing table. Depending on the implementation, this can be as high as six routes. Some implementations require that all routes that are inserted in the routing table have the same metric, while others allow unequal metric routing. In cases where the metric for all installed routes are the same, the router will load balance traffic evenly across each path. When the metric for multiple routes vary, the traffic is load balanced in proportion to the metric (in other words, if one path is “twice as good” as another, two-thirds of the traffic travels down the good path, and one-third of the traffic selects the other one). Asymmetric routing is suboptimal for voice, so route-caching (described earlier) should be considered in this environment.

In addition to using all (up to 6) active paths and optimally using available bandwidth, multipath routing greatly improves convergence time. As soon as a router detects a path failure, it remove it from the routing table, and sends all traffic over the remaining links. If this is a physical link failure, the detection time is nearly instantaneous. Therefore, Avaya recommends the use of multipath routing, where available, across multiple links to a particular location.

Dial backup

One cost-effective technique for installing backup WAN links is to use dial backup. This can be done using either ISDN-BRI or analog lines. ISDN lines typically take 2 seconds to connect, while 56-k analog modems take approximately 1 minute. While this strategy is effective for data traffic, it is less effective for voice. First, the bandwidth may have been greatly reduced. If this is the case, the number of voice channels that can be supported might have been reduced proportionally. Also, if QoS is not properly applied to the backup interface, high packet loss and jitter can adversely affect voice quality. Finally, the time that is required to establish the new link can be up to 1 minute, which disrupts active calls. However, providing that these considerations are taken into account, proper QoS is applied, and a compressed codec is chosen, dial backup can be an effective solution for two to four users.

Convergence times

Convergence is the time that it takes from the instant a failure occurs in the network until a new path through the network is discovered, and all routers or switches are aware of the new path. Convergence times vary, based on the complexity and size of a network. Table 62: Sample convergence times (single link failure) on page 343 lists some sample convergence times that are based on a single link failing in a relatively simple network. They reflect update and/or hello timers expiring. Dialup “convergence” times reflect the time that it takes to dial, connect, and authenticate a connection. These times do not take into account LAG, fast spanning tree, or multipath routing, which speed up convergence. This table shows the importance of carefully planning for fail-over in a network. For example, both OSPF and EIGRP (Layer 3) protocols converge faster than spanning tree (Layer 2). When designing a highly available data network, it is more advantageous to use Layer 3 protocols, especially link-state (OSPF) or hybrid (EIGRP) protocols, than Layer 2 (spanning tree).

Table 62: Sample convergence times (single link failure)

Protocol	Approximate convergence time (seconds)
EIGRP (Cisco)	2
OSPF	6 to 46
RIP	210
Spanning tree (Layer 2)	50+
ISDN dialup (connect + authentication)	2
56-k dialup (connect + authentication)	60

The Converged Network Analyzer

The Converged Network Analyzer (CNA) is an offer from the Avaya Application Assurance Networking (AAN) line of products. It provides two principal value propositions:

- visibility
- path optimization.

Visibility is achieved through the use of real time measurements of the network infrastructure. These measurements feed extensive reports and diagnostics tool, which give the user powerful capabilities. On one end of the spectrum, CNA enables the user to monitor the general health of their network and its ability to support demanding applications such as voice, video, and real time TCP applications. On the other end of the spectrum, CNA enables the user to troubleshoot the cause of a specific network problem.

Path optimization functions as follows: when two paths or more are available between two measured end points, CNA can measure all of the available paths simultaneously. If any problem is detected on one of the paths, CNA can intervene in real time and send route updates to the edge routers, moving the traffic to a non-impaired path. The result is unaffected user experience in the face of network outages.

CNA features a range of application models that assess network conditions. The models focus on the specific characteristics and requirements of different applications:

- Voice
- Video Conferencing
- Video Streaming
- Web applications
- Enterprise TCP applications

Using these application models, CNA translates the performance characteristics of the network path (e.g., latency, jitter, and loss) into Application Performance Ratings (APR). The APRs provide a relative measure of performance if the application were run over this network fabric.

In addition, CNA automatically discovers applications running over the network and can optionally measure load over various links in the network. A sophisticated policy language allows the user to specify precise policies in terms of:

- What applications to optimize
- The performance level to maintain for these applications
- The preferred paths through which to send traffic for these applications
- Load thresholds not to exceed on specific paths.

The CNA package comprises servers that perform most of the analysis, provide the path optimization functionality, and store the reports. CNA also comprises optional no cost test agents that are embedded in an array of avaya phones, gateways, and Avaya partner products

such as Extreme Networks (http://www.extremenetworks.com/homepage.asp). Test agents are also available in low cost devices that can be deployed standalone. Test agents help complement server measurements in two ways: they allow end to end measurement to be performed between specific points of interest (such as phones, gateways, or video conferencing end points); and they provide a view of network impairments over a full mesh of paths between the various sites of an enterprise.

The visibility and path optimization value propositions provided by CNA are instrumental to IP Telephony. VoIP is a real time application with stringent requirements: delay, loss, and jitter effects over the network can affect voice traffic and destroy the user experience. CNA can provide both visibility into such network impairments and means to troubleshoot their cause. Using the CNA Voice application model, network measurements can be translated into an application score that describes the ability of the network fabric to support the IPT application. The Application Score uses a 0 to 5 scale, and can easily be interpreted by IT experts and executives alike. Using the CNA path optimization capabilities, the user can dramatically reduce the effect of network impairments on the voice application running over the network; hence significantly improve the voice communication experience. Finally, CNA can enable IT personnel to specify precise policies that describe the preferred links for voice traffic to use, thresholds on the quality of the voice experience, and load thresholds over given links that need not be exceeded.

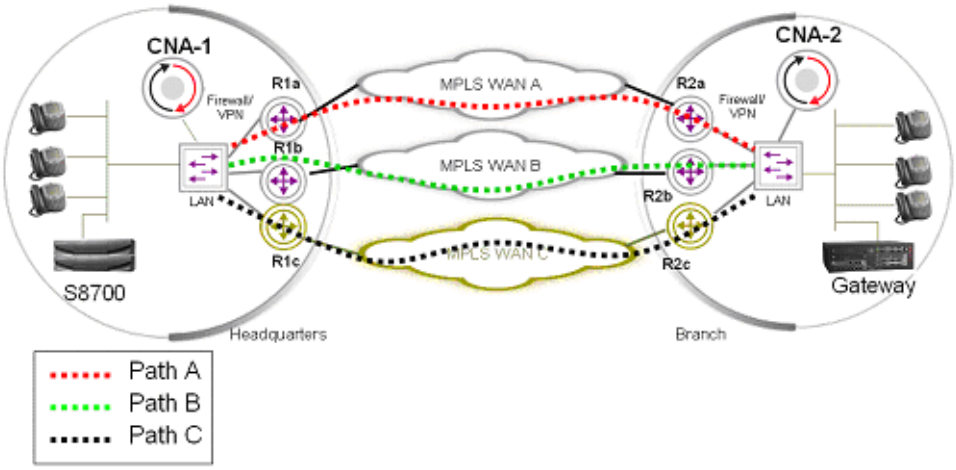
Using the embedded test agents in Avaya phones can significantly augment the value that can be obtained from a CNA deployment. Embedded test agents in end points would allow those end points to measure between each other, hence providing the CNA server with the specific view of the network performance between them. The test agent is embedded in Avaya phones and gateways today. The test agent is also embedded in Extreme Networks products that are GA today: the Summit X450, the BlackDiamond 8800, and the BlackDiamond 10808 switches (http://www.extremenetworks.com/products).

CNA path optimization can also be used to protect signaling traffic. In a typical enterprise, the communication system comprises gateways deployed in a large portion of the enterprise's sites (including many of the small sites) and call controllers running Communication Manager in the regional sites. Phones in the small sites register with the CLANs on the local gateways' port networks; IPSIs on the port networks, in turn, communicate across the WAN with the call controller through a IPSI connection over what is referred to as a control network. This IPSI connection is critical, as it allows phones to communicate with the call controller, pass to it critical stimuli such as depressed digits, access features offered by the call controller, and have the call controller provide dial tone to the phone. An IPSI connection carries as many links as there are active phone calls utilizing the connection. Given the critical nature of the IPSI, any outage in the IPSI connection path can trigger an aggressive recovery mechanism which could result in intermittent feature loss or dropped calls, depending on the severity of the outage. IPSI connection loss can be prevented using CNA path optimization.

CNA path optimization requires path diversity, which is a key to WAN resiliency. Through the provisioning of two or more diverse paths, the enterprise is not at the mercy of failures affecting one of the paths. For example, consider Figure 93. Assume that the current connection between the headquarter and the branch site is through Path A. Assuming that an outage affects a portion of the path along Path A, then in principle, dynamic routing protocols should detect the outage and propagate routing updates to the edge routers on the headquarters' side

(Routers R1a, R1b, R1c), and on the branch side (R2a, R2b, and R2c); these routers would then have been able move the traffic to Path B or Path C. In practice, however, some dynamic routing protocols such as Border Gateway Protocols (BGP) are slow to propagate routes. In other instances, network paths involve tunneling, and consequently, layered routing protocols. Consequently, routing updates can take in the order of 30 seconds to reach the edge routers, with negative effects on voice bearer and signaling traffic.

Figure 93: Enterprise example: headquarters and branch connected using 3 diverse paths



CNA components

The Converged Network Analyzer software provides the layer of intelligence that alleviates the problems described above. Through the use of continuous measurements of all available paths, CNA can detect outages in real time. CNA can then send a BGP update to a router that it controls, causing this router to move the traffic in real time. All in all, CNA can redirect an IPSI connection away from an outaged path in less then one second.

CNA is a network appliance that provides the following capabilities:

- Measurements of targets at a rate of multiple packets a second.
- Ability to control routers through a BGP connection to the routers

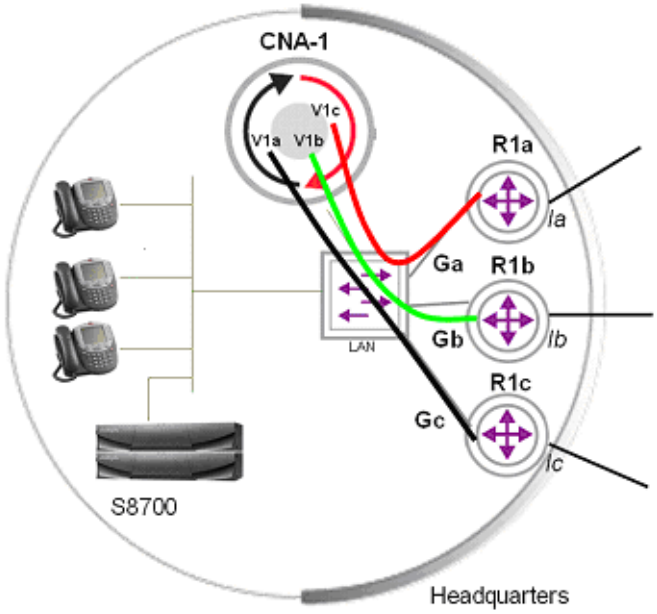
As is shown in Figure 93, CNA is deployed out of line, in the vicinity of the edge routers. Figure 1 shows a scenario where two CNA systems are deployed, one on the headquarters side (CNA-1) and one on the branch side (CNA-2). CNA-1 will simultaneously measure Paths A, B, and C. If an outage affects a portion of the path along Path A, CNA-1 will detect the outage in real time. As soon as the outage is detected, CNA-1 will send a route update to Routers R1a, R1b, and R1c in real time. Similarly, CNA-2 will detect the outage and send a route update to Routers R2a, R2b, and R2c. As a result, the traffic pertaining to the IPSI connection between

Sites A and B will move away from the outage in less than a second, preventing unintelligibility in the audio bearer, or outages in the voice signaling.

Simultaneous monitoring of all paths

The ability for CNA to measure all paths simultaneously is achieved by configuring Policy Based Routing (PBR) functionality on the edge routers. Essentially, measurements through the various links are sourced from different Virtual IP addresses (VIPs). The edge routers are then configured to route the measurement packets to its different links according to the packets' source address. PBR functionality exists in most routers, sometimes under a different name. In Juniper devices, PBR functionality is called Filter-Based Forwarding (FBF).

Figure 94: Headquarters CNA deployment – Measurement plane



In Figure 94, three loopback addresses V1a, V1b, and V1c will be configured on CNA-1. Three Generic Routing Ecapsulation (GRE) tunnels Ga, Gb, and Gc can be configured between the CNA system and the edge routers R1a, R1b, and R1c. Measurement traffic pertaining to Paths A, B, and C will be sourced from V1a, V1b, and V1c, and routed through Ga, Gb, and Gc, respectively. The router will be configured to route traffic emerging from Ga, Gb, and Gc to interfaces Ia, Ib, and Ic respectively.

The GRE tunnels allow the measurement traffic to emerge from their own virtual interfaces on the routers. This way, PBR rules can be made to apply on those virtual interfaces only. This setup presents advantages in some contexts, especially when the edge routers are unable to perform line rate PBR. In such contexts, applying PBR rules to the measurement traffic only helps prevent performance degradation. An alternative to building GRE tunnels is to configure different VLANs for each of the measurement streams.

Controlling edge routers

CNA maintains a BGP peering with every edge device it needs to control. It is configured as a route reflector to the edge devices, which allows it to (1) receive state of the routing table from the edge devices, and (2) send BGP control messages to the edge routers pertaining to destinations it needs to control. The edge routers need to be configured so that route updates from CNA are given priority over other route updates regarding the same destinations. This is accomplished by giving either a higher Weight or a higher LOCAL PREF to updates coming from CNA. If given higher Weights, the route updates' high priority status will only apply on the edge routers themselves. If given higher LOCAL PREF, then the high priority status of these route updates will apply across the entire Autonomous System.

Some router vendors, such as Juniper don't support weight. For routers from those vendors, LOCAL PREF is used to give high priority to routes updates sent by CNA.

In the scenario shown in Figure 94: Headquarters CNA deployment – Measurement plane on page 347, CNA-1 and CNA-2 would be configured as route reflectors to Routers R1a, R1b, and R1c respectively. Routers R1a, R1b and R1c would be configured to apply higher LOCAL PREF to updates received from CNA-1 and CNA-2, respectively. When CNA-1 sends a route update to R1a, the route update will win and traffic will be routed accordingly; similarly for when CNA-1 sends a route update to R1b.

Translating low level statistics to an Application Performance rating

See CNA Application Performance Rating on page 254 for a description of the CNA Application Performance rating (APR) based on application models.

Signaling traffic uses TCP and consists of short transactions. The CNA application model that best captures the characteristics of signaling traffic is the enterprise application model. The enterprise application model takes into account the impact of delay and loss on the TCP transport protocol. It also assumes short transactions and uses transaction delay as the measure of performance, which is translated into the 0-5 Application Performance rating.

Configuration and deployment details

Appendix A: CNA configuration and deployment on page 359 provides detailed procedures for configuring CNA.

Network assessment offer

Avaya Communication Solutions and Integration (CSI) supports a portfolio of consulting and engineering offers to help plan and design:

- IP Telephony
- Data Networking Services
- Network Security Services.

How to contact the CSI

- On the Web — CSI
- E-Mail: bcsius@avaya.com
- Phone: +1 866-282-9266

See the IP Network Readiness Assessment Policy web page for information about the network assessment service.

Problems with data networks

Many customer IP infrastructures appear to be stable and perform at an acceptable levels but have performance and stability issues that create problems for Avaya IP Telephony. While the customer network appears to be ready for full-duplex IP Telephony, Avaya cannot assure performance and quality without a Network Assessment.

Avaya network readiness assessment services

The Network Readiness Assessment Services for Avaya IP Telephony consist of 2 phases:

- Basic network readiness assessment service is a high-level LAN/WAN infrastructure evaluation that determines the suitability of an existing network for IP Telephony.

  The Basic Report includes detailed technical information about any problems that are discovered in the customer infrastructure. It also includes performance predictions based on network and system administration standards.

  If the survey discovers significant network issues, these must be remedied before deploying any Avaya IP Solution. Customers can resolve the problems independently and follow up with another Basic Report (at an additional charge) or to move ahead with the Detailed network readiness assessment service.

Note:

The Basic Network Readiness Assessment Service is available in the U.S. and Canada through direct and indirect channels.

- Detailed network readiness assessment service is typically the second phase in the Network Assessment for IP Telephony solutions. The Detailed network readiness assessment service takes information gathered from the Basic Report, performs problem diagnosis and provides functional requirements for the network to implement Avaya IP Telephony.

  A Detailed network readiness assessment service is required when the Basic Report indicates that the customer's network as it is configured cannot support the proposed IP Telephony application at the desired performance levels. Sometimes customers already know that their existing network is not configured to support Avaya IP Telephony, and they can order a Detailed network readiness assessment service without first completing a Basic Report. The assessment requires that the customer complete a Basic-like analysis as the first phase). Customers may also request a Detailed network readiness assessment service to optimize their network.

Basic network readiness assessment service

The Basic Network Readiness Assessment Service is a scheduled remote network evaluation that is valuable for all customers that are expanding their communication capabilities.

The Basic service evaluates the customer's current network environment by

- Maximizing the available resources.
- Identifying additional resources that are required to support the proposed IP Solution.

The outcome of the Basic service is a road map that identifies the gaps in the existing network today, but it does not provide step-by-step configuration instructions on how to deploy the solution. The Basic service is performed remotely and must be scheduled with the CSI team 2 weeks before implementing Avaya IP Telephony.

What if my network functions well today?

Even if your network appears to perform acceptably, IP Telephony taxes network resources and performance because IP Telephony requires dedicated bandwidth and is more sensitive to network problems than data applications. Table 63: Basic Network Readiness Assessment Service components on page 351 shows the Basic service components and the depth of Avaya's network analyses.

Table 63: Basic Network Readiness Assessment Service components

Component	Who does this?	What does this do? What are the results?	What happens with the results?
Network Topology Report	Customer	Describes your network configuration.	Topology report integrated with all other Basic service components.
Site Configuration Survey	Customer	Data for individual customer site; high-level health check.[1]	Professional Service (PS) engineer reviews data and recommends where to deploy Protocol Analysis software.
Vital Agent analysis	Customer downloads application to identified desktops	Vital Agent collects data about the customer's network traffic.	PS Engineer analyzes the traffic data and determines where to deploy the Performance Analysis software.
Protocol Analysis	Avaya	Measures the data exchange between the local host and remote resources and tests the current load for appropriate bandwidth.	Deeper data analysis (CSI engineer)

1. If the network fails to meet the minimum criteria required for network throughput, configuration, or additional resources are needed, Avaya recommends the more in-depth analysis of the Detailed network readiness assessment service.

Site Configuration Survey

The ECLIPS Site Configuration Survey (SCS) is an detailed customer-view of the their network. This survey is required as part of the Customer Infrastructure Readiness Survey process. The ECLIPS SCS questionnaire must be filled out as completely as possible, and can require the Account Team's regional Sales Engineering resources to assist. In addition to the SCS the customer must provide a topology map of their existing network (LAN/WAN and hardware/ software configuration listings). When the SCS is complete, the customer provides both the SCS and Topology Maps with detailed descriptions of topology components (routers, Ethernet switches, PSTN linked systems, firewalls, servers, E-mail systems, etc.). This information goes to the CVDN Professional Service engineering team that reviews this information and prepares for the Vital Agent Analysis, the second component of the Basic network readiness assessment service.

Vital Agent analysis

Vital Agent is a high-level analysis tool that passively monitors and reports throughput and performance statistics and errors and reports any problems that the host computer encounters. The customer must install and run the Vital Agent software on all desktops targeted for Avaya IP Telephony.

If the customer has a somewhat standardized network infrastructure, Avaya can waive the need to install this application on every desktop and instead to run this utility only on key desktops.

The Vital Agent software gathers data for up to 5 consecutive business days after which the customer sends the data file to the CVDN Professional Service engineers for analysis. The CVDN then determines if the proposed Avaya IP Telephony application can perform acceptably over the customer's network.

If a problem is uncovered as a result of the survey, the CVDN Professional Service engineering team notifies the Account Team and includes detailed technical information regarding the problem. The customer has two choices:

- Resolve the problems independently and then re-run the survey afterward;
- Hire Avaya to perform an on-site Detailed network readiness assessment service.

Detailed network readiness assessment service

The Detailed network readiness assessment service includes

- Scheduled on-site evaluations
- Traffic simulation
- Network testing
- Analysis of the results
- Recommendations to resolve any network throughput issues

In order to reap the benefits of IP Telephony, customers must either possess or acquire a keen understanding of their network and its performance capabilities. This ensures that the transfer of information between systems and processes is not compromised and that the network infrastructure remains stable.

The Detailed service results are documented in a Network Assessment Report that identifies the root cause of the network issues and provides the customer with recommendations on how to resolve those issues to support the implementation of the IP Telephony solution. CVDN Professional Services utilizes proven methodologies performed by a staff of highly-experienced, certified network engineers. These engineers are capable of addressing the customer's critical business needs in complex, multimedia, and multivendor environments.

Use these links for more information about the Detailed network readiness assessment service components:

The Detailed network readiness assessment process

To begin the Detailed network readiness assessment process, the customer must have completed the:

- Basic network readiness assessment service. If a customer has already concluded that their network is not ready for the implementation of Avaya IP Telephony, they can skip the Basic service.
- Site Configuration Survey (SCS).
- Network topology map.

During a Detailed network readiness assessment service, data collection utilities and network simulation tools are loaded onto a customer's network at pre-determined endpoints. Traffic with similar characteristics injected onto the network and monitored for performance under load conditions. After the performance analysis, a comprehensive report documenting network performance, problem areas, and suggested resolutions is given to the customer. The CVDN Professional Services organization can also provide a separate proposal to assist the customer in configuration and integration/administration engineering services to prepare the network for the proposed Avaya IP Telephony application.

Table 64: Detailed network readiness assessment service components on page 354 shows the Detailed network readiness assessment service components and the information exchange between Avaya and the customer.

Table 64: Detailed network readiness assessment service components

Component	Who does this?	What does this do? What are the results?	What happens with the results?
Network Topology Report	Customer (may already be part of Basic service)	Describes your network configuration.	Topology report integrated with all other Detailed service components.
Site Configuration Survey	Customer (can already be part of Basic service)	Data for individual customer site; high-level health check.	Professional Service (PS) engineer reviews data and recommends where to deploy Protocol Analysis software.
Traffic Injection Monitoring Data Collection	Avaya	Determines endpoints (with SNMP agents installed) for data collection. Monitors each network segment for busy hour traffic	Data analyzed to determine the highest level phone quality (starting at 64Kbps) and working through lower quality levels.
Additional tests	Avaya	Summary of Impact of Delay	
		Packet Loss and Jitter on Quality of Service on Voice Quality	
		Summary of Quality using Avaya's Specification for Delay, Loss, and Jitter	
		Impact of Quality of Service on Voice Quality	
		Summary of Quality of Real World Pilot	Summarizes the entire network analysis.
		Layer 3 Traffic Analysis	

Customer responsibilities

In order to successfully complete a Detailed network readiness assessment the customer must:

- Provide technical resource personnel who are well-versed in the network infrastructure.
- Provide complete access to the network.
- Provide passwords for networking equipment.
- Provide access to personnel for interviews.
- Update or provide network topology maps.
- Identify a place on the network for test equipment.
- Define times to complete network testing.

Discovery

- Perform interviews with IT staff to determine application and network performance expectations
- Locate and identify all SNMP enabled devices
- Identify hosts on each subnet
- Identify all routers, switches, and hubs
- Manual identification of all non-SNMP enabled devices
- Identify operating system of each Host found
- Map hosts to communication paths between hosts
- Generate Layer 3 topology map to compare with Basic service
- Install endpoints for testing
- Review WAN-specific circuits, bandwidths, DLCI/PVC configurations, and channeled T1 configurations
- Review the customer’s Layer 2 architecture

Element monitoring

- Monitor router status through SNMP (port utilization, MIB II errors)
- Capture all network device SNMP data real-time into database
- CPU utilization capturing per host being used for testing
- Monitor LAN switch utilization, MIB II errors

Synthetic IP Telephony measurements

- Inject busy hour IP Telephony call traffic simulation into live network segments
- Random CODECs and injection points between pre-defined end points/hosts
- Injections initially within single facilities, replicated across WAN end points as appropriate
- Capture of all test data into database real-time

Remote analysis

- Analysis of element/endpoint data by router, time period, and other performance variables
- Analysis of element/endpoint data by switch, time period, other performance variables
- Analysis of IP Telephony call data by IP endpoint pair, time period, and other performance variables, then integrated with SNMP data
- Generation of graphs representing usage for all endpoint data
- “What if” analysis of IP Telephony codecs to determine best match for performance and call quality

Report generation

- Summary of IT and Voice team’s interviews: perceived expectations and requirements as related to proposed applications and network performance levels
- Physical topology map on all devices discovered and monitored on the network
- Analysis of WAN circuits: current status and recommendations for support of proposed Avaya IP Telephony
- Traffic analysis reports, including archive on CD-ROM of all captured data for all segments monitored and injected with simulated busy hour IP Telephony calls
- Recommendations of Avaya Engineering team to resolve infrastructure problems discovered and/or make-ready for proposed Avaya IP Telephony
- Summary reports of segment utilization, errors, and dropped packets
- Summary E-Model calculations for different CODEC reports per segment/per layer
- Summary reports for the Level 3 QoS audits (if performed)
- Summary reports for different network layers’ performance

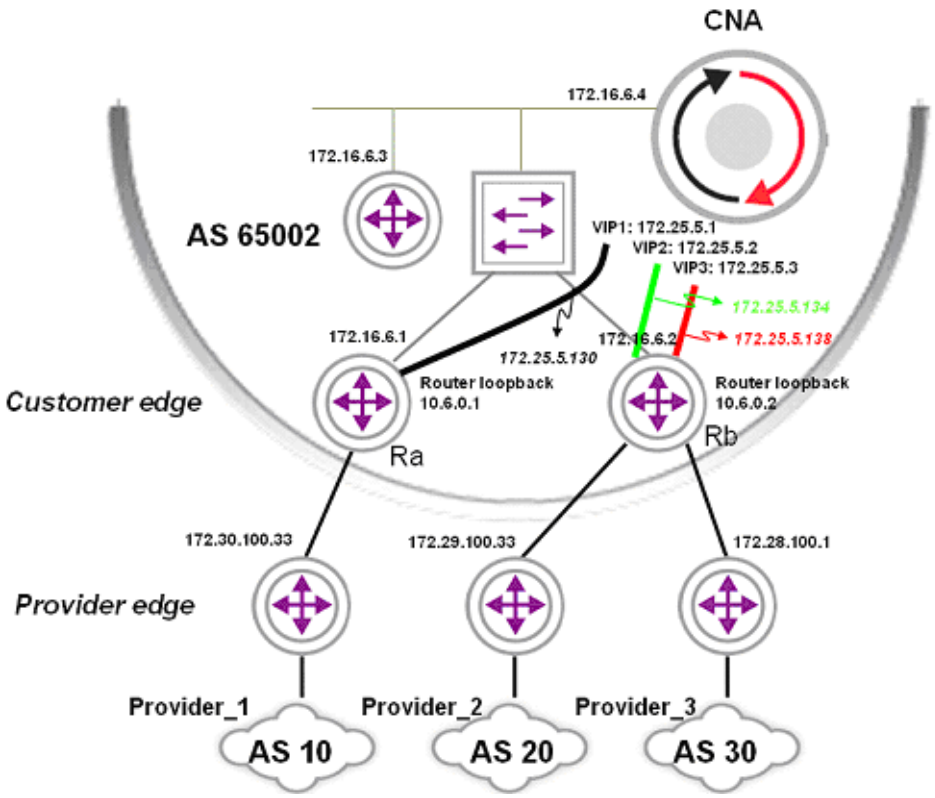
Customer deliverables

- Avaya networking experts perform discovery of the customer's network and document findings in a Detailed Network Readiness Assessment Report delivered to the customer.
- Accurate network topology
- Measurements of actual usability performance levels, throughput performance of the LAN, and server utilization
- Results of traffic simulation on the network at projected volumes
- Define problem areas, causes, and functional requirement recommendations to be implemented in the network design

Appendix A: CNA configuration and deployment

This section provides detailed CNA configuration procedures for the scenario shown in Figure 95. For the purpose of generality, we assume two routers and three paths.

Figure 95: Detailed configuration scenario



Configuring CNA

Basic configuration

Configuring Virtual Module Interfaces

Avaya CNA Ethernet interfaces need to be associated with an Ethernet interface and a physical connection to the network. Once the system has booted and all of its necessary ports are connected to the network, a terminal or workstation can be connected to the serial console port on the CNA system.

Using privileged-level access, the user should enter the **`configure terminal`** command.

Ethernet Interfaces on Modules

To create an interface, enter the interface command while in config mode. Enter *`fastethernet`* as the *`type`* argument. The *`num argument`* is *`0`*, while the *`port`* arguments correspond with the labeled Ethernet ports on the system.

To assign an address to the interface, enter the ip address command with a valid IP address and mask from your network address space. End the configuration of this interface with the end command. E.g., for the management interface, enter the command to configure Ethernet 0. Ustat modules will also have to be referred to inside the interface module. (Ustat modules will be defined on Page 9).

```
interface fastethernet 0/0
  ip address 176.16.6.4 255.255.255.224
  module ustat provider_1
  module ustat provider_2
  module ustat provider_3
end
```

Default Gateway

A default route needs to be defined for the system so that it knows how to communicate with the rest of the network:

```
ip route 0.0.0.0 0.0.0.0 172.16.6.3
```

Service Provider Access Links

Each service provider that is to be managed or monitored by Avaya CNA needs a link object defined. From config mode, enter engine configuration mode:

```
module engine
```

To associate a service provider with a link name, create the links using the **link** command.

```
link provider_1
  provider-as 10 172.30.100.33
end
link provider_2
provider-as 20 172.29.100.33
end
link provider_3
provider-as 30 172.28.100.1
end
```

The name provider_1 will be used in the output of various CLI commands and web page reports. The provider-as command associates the provider_1 link with both the Autonomous System (AS) number of the corresponding service provider; and the IP address of the provider edge the enterprise's edge router is peering with.

BGP on the Engine Module

While still in config-engine mode, enter the bgp command, with the enterprise network's AS number as the as-num argument:

```
bgp 65002
  neighbor 172.16.6.1 link provider_1
  neighbor 172.16.6.1 remote-as 65002
  neighbor 172.16.6.2 link provider_2
  neighbor 172.16.6.2 link provider_3
  neighbor 172.16.6.2 remote-as 65002
end
```

A neighbor link command needs to be entered once for each of the links. The command takes address and name arguments, in the following form: The address argument is the IP address of an interface on the edge router that connects the enterprise network to the service provider identified by the name argument.

Also, in order to achieve IBGP peering, the router IP addresses need to be associated with the enterprise's AS numbers, using the neighbor remote-as command.

Assigning USTATs to Providers

*module usta*t commands now need to be defined for each WAN link:

```
module ustat provider_1
  link provider_1
  vip 172.25.5.1
```

The ustat module specifies the association of the USTAT module to a specific WAN link and the virtual IP (VIP) address to this WAN link.

USTAT GRE Tunnels

To configure GRE Tunnels for measurements, use the interface tunnel command, then assign the tunnel to a ustat:

```
interface tunnel 1
  ip address 172.25.5.130 255.255.255.252
  tunnel destination 10.6.0.1
end
module ustat provider_1
  ip route 10.6.0.1 255.255.255.255 172.16.6.1
  ip route 0.0.0.0 0.0.0.0 tunnel1
end
```

Measurements

In this scenario, we'll assume that CNA will only measure to and optimize signaling and bearer targets. We create an address group that contains all signaling targets. We also create an address group that contains all bearer targets. Then, we create within the engine module active measurement groups for the signaling and bearer targets, respectively. The respective groups of addresses are added to the list of targets within the measurement group. The measurement type, rate, and loss timeout are also specified. It is recommended that high measurement rate of 5 per second, and an aggressive timeout (200 ms) are used, to insure sub-second rescue times.

```
group signaling_targets
  Prefix signaling_1/32
  Prefix signaling_2/32
end
group bearer_targets
```

```
  Prefix bearer_1/32
  Prefix bearer_2/32
end
module engine
  active-measurement group AM_signaling_targets
    type icmp
    rate 5 per-second
    timeout 200
    target group bearer_targets
  end
  active-measurement group AM_bearer_targets
    type icmp
    rate 5 per-second
    timeout 200
    target group bearer_targets
  end
end
```

Decision making

Decision making related commands include:

- turning route optimization on
- specifying a decision policy that includes policy preferences and the appropriate application model
- applying the decision policy to the corresponding active measurement group

It is also recommended to insure that when no performance problems are detected, CNA servers on both ends settle on a different link. To get this behavior, one must specify a priority under the link command and disable “damped-mode” within the decision policy.

```
module engine
  damped-mode disable
  link provider_1
    winner-set-priority prefer
  end
  route-assert-mode enable
```

```
  route-assert-filter force
  decision-policy DP_signaling_targets
    set-application-model enterprise
    damped-mode disable
  end
  decision-policy DP_bearer_targets
    set-application-model voice
    damped-mode disable
  end
  set-decision-policy DM_signaling_targets active-measurement-group
  AM_signaling_targets
  set-decision-policy DM_bearer_targets active-measurement-group
  AM_bearer_targets
end
```

Configuring the Routers

The following needs to be added to the enterprise edge routers:

- GRE tunnel interfaces that will connect to the USTAT modules
- route maps for policy routing on the tunnels
- outing between the edge routers and the CNA system, including iBGP peering and
- routing to the USTAT VIPs

For the purposes of describing the CNA configuration process using widely understood terminology, this documentation assumes a simple, generic network that uses Cisco equipment as its edge routers and Cisco IOS commands.

Edge Router GRE Tunnel Interfaces

Each CNA USTAT module needs to be associated with a different tunnel interface on the Cisco router. Referring back to the example in Figure 95, three tunnels are needed. Since there are three USTAT modules and only two edge routers, two of the tunnels—Tunnel1 and Tunnel2—will be created on the one edge router, while the third tunnel—Tunnel3—will be created on the other edge router.

These are the IOS commands needed to set up the GRE tunnel interface on Ra (see Figure 95):

```
interface Tunnel1
description GRE to provider_1
ip address 172.25.5.129 255.255.255.252
ip policy route-map provider_1
tunnel source 172.16.6.1
tunnel destination 172.16.6.4
```

Specifically, here's what the Cisco commands above do:

- the interface command identifies the tunnel to be created—Tunnel1
- the description command adds the text "GRE to provider_1" to the tunnel configuration
- the ip address command identifies the tunnel IP address as 172.25.5.129 255.255.255.252; this address should be in the same network as the tunnel IP address specified on the CNA configuration—172.25.5.130 255.255.255.252
- the ip policy command identifies the route map to be used, which we have called provider_1 (which will be created below, on Page 12); the route map will ensure that traffic from a given USTAT will be directed to the correct WAN link
- the tunnel source command designates the address of the physical interface on the edge router—172.16.6.1 (Cisco IOS syntax requires that it be explicitly specified; CNA syntax has no such requirement—the address is implicitly set to the eth0 interface address of the USTAT module)
- the tunnel destination command identifies the physical address on the USTAT module

These commands will have to be repeated for each GRE tunnel (one for each USTAT module). In this example, the remaining two GRE tunnels will have to be configured on Router Rb. (See Figure 95.)

Route Maps

The tunnel configuration in the previous section referred to a route map called *provider_1*, which is created here, along an access list to restrict entry.

Specify the USTAT module's VIP address in the access list:

```
ip access list 188 permit ip host 172.25.5.1 any
route-map provider_1 permit 10
match ip address 188
set ip next-hop 172.30.100.33
```

The USTAT module's VIP address is specified in the access list. The name of the route map, provider_1, must match exactly the name used in the ip policy command when the GRE tunnel interface was created. The set ip next-hop command should point to the address used to access the ISP being monitored by this USTAT (provider_1, as shown in Figure 95).

These commands will have to be repeated for each USTAT module/ISP pair; at which point the configuration would model the network shown in Figure 95.

Routing Configuration

Here, the routing to the USTAT VIPS are configured; the IBGP peering between the edge router and the CNA system is also configured

VIP Routing:

USTAT modules do not support dynamic routing protocols, so static routes will be used. On each edge router, you static routes are created to each of the CNA tunnels configured on that router.

In global config mode on the edge router Ra, the following Cisco IOS command is used:

```
ip route 172.25.5.1 255.255.255.255 Tunnel1
```

On the edge router Rb, the following Cisco IOS command is used:

```
ip route 172.25.5.2 255.255.255.255 Tunnel2
ip route 172.25.5.3 255.255.255.255 Tunnel3
```

The addresses are the VIPs assigned to each USTAT. Tunnel1 and Tunnel2 coexist on one edge router; Tunnel3 is alone on the other.

Note:

Note: In order to accommodate asymmetric routing—a situation where a packet destined for USTATa, which is configured for Tunnel1, arrives at router ER2, which is configured for Tunnel2—static routes may need to be redistributed into an interior routing protocol, or additional static routes will have to be placed on each edge router.

IBGP

On the edge router, the router bgp command is used with the enterprise's Autonomous System Number:

```
router bgp 65002
```

Route Reflection

The CNA system must be a route reflector client to all of the edge routers that will operate within the CNA system's sphere of influence. When multiple edge routers are being configured for route reflection, a BGP cluster ID is required. The number can be either a 32 bit integer or an IP address; the same number must be used on each device on which routing tables are to be placed under the direction of the CNA system.

```
bgp cluster-id 88
```

Now the parameters of the IBGP peering configuration from the edge router to the CNA system need to be defined:

```
neighbor 172.16.6.4 remote-as 65002
neighbor 172.16.6.4 description IBGP to CNA
neighbor 172.16.6.4 route-reflector-client
neighbor 172.16.6.4 soft-reconfiguration inbound
neighbor 172.16.6.4 weight 200
```

The IP address used are the same configured on the CNA system. The remote-as command identifies the peering as IBGP (because the remote AS number matches the AS number in the bgp command). The description command adds some descriptive text to the configuration. The route-reflector-client command designates the CNA system as a BGP route reflector client. The soft-reconfiguration command allows the CNA system to make changes to the BGP configuration without a session reset.

The weight command assigns a high value to the CNA system, which causes the edge router to prefer the CNA system's routing assertions over the natural BGP route selection. This assignment is non-transitive, which means that the weighting is not communicated to other IBGP or EBGP peers. The weight attribute is local to this router only. In the example, weight is set to 200. The actual setting will be dependent on the local policies; the weight value should be high enough to prevail over those policies.

Note:

The CNA system has a built-in precaution that prevents its route assertions from leaking beyond your edge router's borders. The no-export attribute is always set in all CNA BGP routing updates. This is not user configurable. This attribute prohibits the router from passing routes that it has learned from the CNA system to routers outside the local AS.

Command summary

All of the CNA and router configuration commands described in this document are listed in this section. For more information, please refer to the CNA administrative guide.

CNA commands

```
interface fastethernet 0/0
  ip address 176.16.6.4 255.255.255.224
  module ustat provider_1
  module ustat provider_2
  module ustat provider_3
end
interface tunnel 1
  ip address 172.25.5.130 255.255.255.252
  tunnel destination 10.6.0.1
end
interface tunnel 2
  ip address 172.25.5.134 255.255.255.252
  tunnel destination 10.6.0.2
end
interface tunnel 3
  ip address 172.25.5.138 255.255.255.252
  tunnel destination 10.6.0.2
end
ip route 0.0.0.0 0.0.0.0 172.16.6.3
group IPSI_targets
  Prefix ISPI_1/32
  Prefix IPSI_2/32
end
module engine
  damped-mode disable
  route-assert-mode enable
```

```
  route-assert-filter force
  link provider_1
    provider-as 10 172.30.100.33
    winner-set-priority prefer
  end
  link provider_2
    provider-as 20 172.29.100.33
  end
  link provider_3
   provider-as 30 172.28.100.1
  end
  bgp 65002
    neighbor 172.16.6.1 link provider_1
    neighbor 172.16.6.1 remote-as 65002
    neighbor 172.16.6.2 link provider_2
    neighbor 172.16.6.2 link provider_3
    neighbor 172.16.6.2 remote-as 65002
  end
  active-measurement group AM_IPSI_targets
    type icmp
    rate 5 per-second
    timeout 200
    target group IPSI_targets
  end
  decision-policy DP_IPSI_targets
    set-application-model enterprise
    damped-mode disable
  end
  set-decision-policy DM_IPSI_targets active-measurement-group
  AM_IPSI_targets
  end
end
module ustat provider_1
  link provider_1
```

```
  vip 172.25.5.1
  ip route 10.6.0.1 255.255.255.255 172.16.6.1
  ip route 0.0.0.0 0.0.0.0 tunnel1
end
module ustat provider_2
  link provider_2
  vip 172.25.5.2
  ip route 10.6.0.2 255.255.255.255 172.16.6.2
  ip route 0.0.0.0 0.0.0.0 tunnel2
end
module ustat provider_3
  link provider_3
  vip 172.25.5.3
  ip route 10.6.0.2 255.255.255.255 172.16.6.2
  ip route 0.0.0.0 0.0.0.0 tunnel3
end
```

Router Ra commands

```
interface Tunnel1
  description GRE to provider_1
  ip address 172.25.5.129 255.255.255.252
  ip policy route-map provider_1
  tunnel source 172.16.6.1
  tunnel destination 172.16.6.4
ip access list 188 permit ip host 172.25.5.1 any
route-map provider_1 permit 10
  match ip address 188
  set ip next-hop 172.30.100.33
ip route 172.25.5.1 255.255.255.255 Tunnel1
router bgp 65002
  bgp cluster-id 88
  neighbor 172.16.6.4 remote-as 65002
  neighbor 172.16.6.4 description IBGP to CNA
```

```
  neighbor 172.16.6.4 route-reflector-client
  neighbor 172.16.6.4 soft-reconfiguration inbound
  neighbor 172.16.6.4 weight 200
```

Router Rb commands

```
interface Tunnel2
  description GRE to provider_2
  ip address 172.25.5.133 255.255.255.252
  ip policy route-map provider_2
  tunnel source 172.16.6.2
  tunnel destination 172.16.6.4
interface Tunnel3
  description GRE to provider_3
  ip address 172.25.5.137 255.255.255.252
  ip policy route-map provider_3
  tunnel source 172.16.6.2
  tunnel destination 172.16.6.4
ip access list 189 permit ip host 172.25.5.2 any route-map provider_2
permit 20
  match ip address 189
  set ip next-hop 172.29.100.33
ip access list 190 permit ip host 172.25.5.3 any route-map provider_3
permit 30
  match ip address 190
  set ip next-hop 172.28.100.1
ip route 172.25.5.2 255.255.255.255 Tunnel2
ip route 172.25.5.3 255.255.255.255 Tunnel3
router bgp 65002
  bgp cluster-id 88
  neighbor 172.16.6.4 remote-as 65002
  neighbor 172.16.6.4 description IBGP to CNA
  neighbor 172.16.6.4 route-reflector-client
  neighbor 172.16.6.4 soft-reconfiguration inbound
  neighbor 172.16.6.4 weight 200
```

This completes the CNA configuration for the scenario referenced in Figure 95: Detailed configuration scenario on page 359.

Index

Numerical

A

B

C

D

E

F

G

H

I

J

L

M

N

P

Q

R

S

T

U

V

W

X